ESET

REMOTE ADMINISTRATOR 6

Manuale di installazione e dell'utente

Fare clic qui per accedere alla versione più recente di questo documento

ENJOY SAFER TECHNOLOGY™

ESET **REMOTE ADMINISTRATOR 6**

Copyright © 2015 **di ESET, spol. s r.o.**
ESET Remote Administrator 6 è stato sviluppato da ESET, spol. s r.o.

Per ulteriori informazioni, visitare il sito Web www.eset.it.
Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.
ESET, spol. s r.o. si riserva il diritto di modificare qualsiasi parte del software dell'applicazione descritta senza alcun preavviso.

Supporto tecnico: www.eset.com/support

REV. 20/05/2015

Contenuti

1. Introduzione....6

1.1 Funzioni....6

1.2 Architettura....7

1.2.1 Server....8
1.2.2 Console Web....9
1.2.3 Agente....9
1.2.4 Proxy....10
1.2.5 Rogue Detection Sensor....11
1.2.6 Connettore dispositivi mobili....12
1.2.7 Scenari di utilizzo....13
1.2.7.1 Server singolo (aziende di piccole dimensioni)....13
1.2.7.2 Diramazioni remote con proxy....14
1.2.7.3 Alta disponibilità (Enterprise)....15
1.2.8 Esempi di utilizzi pratici....16

1.3 Prodotti e lingue supportati....17

2. Requisiti di sistema....19

2.1 Hardware....19

2.2 Database....19

2.3 Sistemi operativi supportati....20

2.3.1 Windows....20
2.3.2 Linux....22
2.3.3 OS X....22

2.4 Porte utilizzate....23

3. Processo di installazione....24

3.1 Installazione pacchetto....25

3.1.1 Installazione su Windows SBS/Essentials....26

3.2 Database....29

3.2.1 Backup del server del database....29
3.2.2 Aggiornamento del server del database....29
3.2.3 Migrazione del database ERA....30
3.2.3.1 Processo di migrazione per SQL Server....30
3.2.3.2 Processo di migrazione per MySQL Server....38

3.3 Immagine ISO....39

3.4 Accessori virtuali....39

3.4.1 VMware Player....42
3.4.2 Oracle VirtualBox....43
3.4.3 Microsoft Hyper-V....44

3.5 Cluster di failover - Windows....45

3.6 Cluster di failover - Linux....45

3.7 Installazione componenti su Windows....48

3.7.1 Installazione server - Windows....48
3.7.1.1 Prerequisiti server - Windows....50
3.7.2 Microsoft SQL Server - Windows....51
3.7.3 Installazione dell'agente - Windows....51
3.7.4 Installazione console Web - Windows....52
3.7.4.1 Browser Web supportati....53
3.7.5 Installazione proxy - Windows....53
3.7.5.1 Prerequisiti proxy - Windows....54
3.7.6 Installazione RD Sensor - Windows....54
3.7.6.1 Prerequisiti RD Sensor - Windows....54
3.7.7 Installazione di Connettore dispositivi mobili - Windows....54
3.7.7.1 Prerequisiti di Connettore dispositivi mobili - Windows....57
3.7.8 Installazione del proxy Apache HTTP - Windows....59

3.8 Installazione componenti su Linux....60

3.8.1 Installazione server - Linux....60
3.8.1.1 Prerequisiti server - Linux....62
3.8.2 Installazione agente - Linux....63
3.8.2.1 Prerequisiti dell'agente - Linux....64
3.8.3 Installazione di ERA Web Console - Linux....65
3.8.3.1 Prerequisiti di ERA Web Console - Linux....65
3.8.4 Installazione proxy - Linux....65
3.8.4.1 Prerequisiti proxy - Linux....66
3.8.5 Installazione e prerequisiti di RD Sensor - Linux....67
3.8.6 Installazione di Connettore dispositivi mobili - Linux....67
3.8.6.1 Prerequisiti di Connettore dispositivi mobili - Linux....69
3.8.7 Installazione del proxy Apache HTTP - Linux....69
3.8.8 Come disinstallare o reinstallare un componente - Linux....72

3.9 Record servizio DNS....73

3.10 Strumento di migrazione....74

3.10.1 Scenario di migrazione 1....75
3.10.2 Scenario di migrazione 2....77
3.10.3 Scenario di migrazione 3....80

4. Primi passi....84

4.1 Aprire ERA Web Console....84

4.2 Schermata di accesso di ERA Web Console....86

4.3 Conoscere ERA Web Console....88

4.4 Distribuzione....90

4.4.1 Aggiungere un computer client alla struttura ERA....91
4.4.1.1 Utilizzo della sincronizzazione Active Directory....91
4.4.1.2 Digitazione manuale nome/IP....92
4.4.1.3 Utilizzo di RD Sensor....93
4.4.2 Distribuzione agente....96
4.4.2.1 Passaggi distribuzione - Windows....96
4.4.2.1.1 Programmi di installazione live dell'agente....97
4.4.2.1.2 Distribuisci agente da remoto....100
4.4.2.1.3 Distribuisci agente localmente....105
4.4.2.2 Passaggi distribuzione - Linux....108
4.4.2.3 Passaggi di distribuzione - OS X....109
4.4.2.4 Risoluzione dei problemi - Distribuzione agente....109
4.4.3 Distribuzione dell'agente mediante GPO e SCCM....111
4.4.3.1 Creare il file MST....111
4.4.3.2 Passaggi di distribuzione - GPO....118
4.4.3.3 Passaggi di distribuzione - SCCM....122
4.4.4 Installazione prodotto....138
4.4.4.1 Installazione prodotto (riga di comando)....141
4.4.4.2 Elenco di problemi quando l'installazione non riesce....142

4.5 Gestione 142
4.5.1 Aggiungi computer ai gruppi 143
4.5.1.1 Gruppi statici 143
4.5.1.1.1 Aggiungi computer a un gruppo statico 144
4.5.1.2 Gruppi dinamici 145
4.5.1.2.1 Nuovo modello gruppo dinamico 146
4.5.1.2.2 Crea nuovo gruppo dinamico 147
4.5.2 Crea un nuovo criterio 149
4.5.3 Assegna un criterio a un gruppo 152
4.5.4 Registrazione dispositivo mobile 154

4.6 Procedure consigliate 156
4.6.1 Gestione utenti 156

5. Utilizzo di ESET Remote Administrator 157

5.1 Dashboard 157
5.1.1 Impostazioni dashboard 159
5.1.2 Drill down 160
5.1.3 Modifica modello di report 161

5.2 Computer 165
5.2.1 Aggiungi computer 167
5.2.2 Dettagli computer 169

5.3 Minacce 170

5.4 Report 171
5.4.1 Crea un nuovo modello di report 172
5.4.2 Genera report 175
5.4.3 Pianifica un report 175
5.4.4 Applicazioni obsolete 175

6. Amministrazione di ESET Remote Administrator 176

6.1 Amministrazione 176
6.1.1 Gruppi 176
6.1.1.1 Crea nuovo gruppo statico 178
6.1.1.2 Crea nuovo gruppo dinamico 181
6.1.1.3 Assegna attività a un gruppo 183
6.1.1.4 Assegna un criterio a un gruppo 184
6.1.1.5 Criteri e gruppi 186
6.1.1.6 Gruppi statici 186
6.1.1.6.1 Procedura guidata gruppo statico 186
6.1.1.6.2 Gestisci gruppi statici 187
6.1.1.6.3 Sposta gruppo statico 188
6.1.1.6.4 Aggiungi computer client a gruppo statico 190
6.1.1.6.5 Importa client da Active Directory 192
6.1.1.6.6 Assegna un'attività a un gruppo statico 192
6.1.1.6.7 Assegna un criterio a un gruppo statico 192
6.1.1.6.8 Esporta gruppi statici 193
6.1.1.6.9 Importa gruppi statici 194
6.1.1.7 Gruppi dinamici 195
6.1.1.7.1 Procedura guidata modello gruppo dinamico 195
6.1.1.7.2 Gestisci modelli gruppi dinamici 196
6.1.1.7.3 Procedura guidata gruppo dinamico 198
6.1.1.7.4 Crea gruppo dinamico tramite il modello esistente 199
6.1.1.7.5 Crea gruppo dinamico tramite nuovo modello 201
6.1.1.7.6 Gestisci gruppi dinamici 201
6.1.1.7.7 Sposta gruppo dinamico 203
6.1.1.7.8 Assegna un criterio a un gruppo dinamico 205
6.1.1.7.9 Assegna un'attività a un gruppo dinamico 205
6.1.1.7.10 Come automatizzare ESET Remote Administrator 205
6.1.1.7.11 Quando un computer diventa un membro di un gruppo dinamico? 206
6.1.1.7.12 Valutazione delle regole del modello 206
6.1.1.7.13 Editor regole 208
6.1.2 Criteri 210
6.1.2.1 Procedura guidata criteri 211
6.1.2.2 Contrassegni 212
6.1.2.3 Gestisci criteri 213
6.1.2.4 Modalità di applicazione dei criteri ai client 216
6.1.2.4.1 Ordinamento dei gruppi 216
6.1.2.4.2 Enumerazione dei criteri 218
6.1.2.4.3 Unione dei criteri 219
6.1.2.5 Configurazione di un prodotto da ERA 219
6.1.2.6 Assegna criterio a gruppo 219
6.1.2.7 Assegna un criterio a un client 221
6.1.3 Attività client 222
6.1.3.1 Procedura guidata attività client 224
6.1.3.2 Gestisci attività client 228
6.1.3.2.1 Controllo su richiesta 230
6.1.3.2.2 Aggiornamento sistema operativo 233
6.1.3.2.3 Gestione quarantena 235
6.1.3.2.4 Reimposta database Rogue Detection Sensor 237
6.1.3.2.5 Aggiornamento componenti amministratore remoto 240
6.1.3.2.6 Reimposta agente clonato 242
6.1.3.2.7 Esegui comando 244
6.1.3.2.8 Esegui script SysInspector 246
6.1.3.2.9 Installazione software 248
6.1.3.2.10 Disinstallazione software 250
6.1.3.2.11 Attivazione prodotto 252
6.1.3.2.12 Richiesta rapporto SysInspector 254
6.1.3.2.13 Carica file in quarantena 256
6.1.3.2.14 Aggiornamento database firme antivirali 258
6.1.3.2.15 Rollback aggiornamento database firme antivirali 260
6.1.3.2.16 Visualizza messaggio 262
6.1.3.2.17 Azioni Anti-Furto 264
6.1.3.2.18 Registrazione dispositivo 266
6.1.3.2.19 Interrompi gestione (disinstallare agente ERA) 280
6.1.3.3 Esporta configurazione prodotti gestiti 283
6.1.3.4 Assegna attività a gruppo 285
6.1.3.5 Assegna attività a uno o più computer 286
6.1.3.6 Pianifica un'attività 288
6.1.3.7 Attivazioni 290
6.1.4 Attività server 290
6.1.4.1 Procedura guidata attività server 290
6.1.4.2 Gestisci attività server 291
6.1.4.2.1 Distribuzione agente 291

Contenuti

6.1.4.2.2 Genera report ... 296
6.1.4.2.3 Sincronizzazione gruppo statico ... 299
6.1.4.2.4 Sincronizzazione gruppo statico - Computer Linux ... 300
6.1.4.3 Pianificazione attività server ... 301
6.1.4.4 Riutilizza attivazione in attività server ... 301
6.1.4.5 Attivazioni ... 302
6.1.4.5.1 Limitazione delle richieste ... 303
6.1.4.5.1.1 Eccessiva sensibilità dell'attivazione ... 306
6.1.4.5.2 Procedura guidata attivazioni server ... 306
6.1.4.5.3 Gestisci attivazioni server ... 306
6.1.4.5.3.1 Eccessiva esecuzione dell'attivazione ... 308
6.1.4.5.3.2 Espressione CRON ... 309
6.1.4.5.4 Gestisci sensibilità attivazioni ... 309
6.1.5 Notifiche ... 311
6.1.5.1 Procedura guidata notifiche ... 312
6.1.5.2 Gestisci notifiche ... 315
6.1.5.3 Come configurare un servizio trap SNMP ... 317
6.1.6 Certificati ... 318
6.1.6.1 Certificati del peer ... 319
6.1.6.1.1 Crea un nuovo certificato tramite l'autorità di certificazione ERA ... 320
6.1.6.1.2 Crea un nuovo certificato tramite un'autorità di certificazione personalizzata ... 321
6.1.6.2 Autorità di certificazione ... 321
6.1.6.2.1 Crea una nuova autorità di certificazione ... 322
6.1.7 Diritti di accesso ... 323
6.1.7.1 Utenti ... 323
6.1.7.1.1 Procedura guidata gruppo di protezione dominio mappato ... 324
6.1.7.1.2 Procedura guidata utente nativo ... 325
6.1.7.1.3 Crea un utente nativo ... 326
6.1.7.1.3.1 Crea nuovo account amministratore ... 327
6.1.7.1.4 Mappa gruppo su gruppo di protezione dominio ... 327
6.1.7.1.5 Assegna utente a un set di autorizzazioni ... 328
6.1.7.2 Set autorizzazioni ... 329
6.1.7.2.1 Procedura guidata set di autorizzazioni ... 330
6.1.7.2.2 Gestisci set di autorizzazioni ... 331
6.1.8 Impostazioni server ... 332
6.1.9 Gestione licenza ... 332
6.1.9.1 Attivazione ... 335

7. Strumento di diagnostica ... 339

8. Glossario ... 340

8.1 Tipi di infiltrazioni ... 340
8.1.1 Virus ... 340
8.1.2 Worm ... 340
8.1.3 Trojan horse ... 341
8.1.4 Rootkit ... 341
8.1.5 Adware ... 341
8.1.6 Spyware ... 342
8.1.7 Applicazioni potenzialmente pericolose ... 342
8.1.8 Applicazioni potenzialmente indesiderate ... 342

9. Domande frequenti ... 343

10. Informazioni su ESET Remote Administrator ... 15

11. Accordo di licenza per l'utente finale (ALUF) ... 16

1. Introduzione

ESET Remote Administrator (ERA) è un'applicazione che consente all'utente di gestire i prodotti ESET sulle workstation client, i server e i dispositivi mobili in un ambiente di rete da una postazione centrale. Il sistema di gestione delle attività integrato di ESET Remote Administrator consente all'utente di installare soluzioni di protezione ESET su computer remoti e di rispondere rapidamente ai nuovi problemi e alle nuove minacce.

ESET Remote Administrator non offre direttamente protezione contro codici dannosi. La protezione dell'ambiente dipende dalla presenza di una soluzione di protezione ESET come ESET Endpoint Security o ESET File Security per Microsoft Windows Server sulle workstation, i server o i dispositivi mobili.

ESET Remote Administrator 6 si basa su due principi fondamentali:

1. **Gestione centralizzata** : l'intera rete può essere configurata, gestita e monitorata da un'unica posizione.
2. **Scalabilità**: il sistema può essere utilizzato in una piccola rete nonché in ambienti aziendali di grandi dimensioni. L'estensione e la scalabilità rappresentano due metodi che garantiscono un agevole adattamento del sistema all'infrastruttura di lavoro.

Le pagine della guida di ESET Remote Administrator offrono all'utente un manuale di gestione completo. Si consiglia di iniziare ad acquisire dimestichezza con i componenti più utilizzati di ESET Remote Administrator:

- Architettura di ESET Remote Administrator
- Processi di installazione e Processi di utilizzo
- Distribuzione agente mediante GPO o SCCM
- Primi passi dopo l'installazione di ESET Remote Administrator
- Conoscere ERA Web Console
- Utilizzo di ESET Remote Administrator
- Amministrazione
- Strumento di migrazione

1.1 Funzioni

Di seguito vengono illustrate alcune funzionalità e capacità completamente nuove presenti nella versione 6:

- Indipendenza dalla piattaforma: ERA Server funziona sia su Windows che su Linux.
- ERA Web Console, ovvero l'interfaccia utente principale di ESET Remote Administrator, è accessibile attraverso il browser Web. Ciò facilita l'utilizzo di questa risorsa da qualsiasi posizione e dispositivo.
- Un Dashboard completamente personalizzabile offre una panoramica straordinaria dello stato di protezione della rete e la sezione Amministrazione di ESET Remote Administrator Web Console (ERA Web Console) è uno strumento efficace e accessibile per la gestione dei prodotti ESET.
- Le Notifiche garantiscono l'invio di informazioni rilevanti in tempo reale e i Report consentono di ordinare in modo pratico vari tipi di dati da utilizzare in momenti successivi.

1.2 Architettura

Per un utilizzo completo del portafoglio di soluzioni di protezione ESET, è necessario installare i seguenti componenti (piattaforma Windows):

- Server ERA
- Database ERA
- ERA Web Console
- Agente ERA

Per un utilizzo completo del portafoglio di soluzioni di protezione ESET, è necessario installare i seguenti componenti (piattaforma Linux):

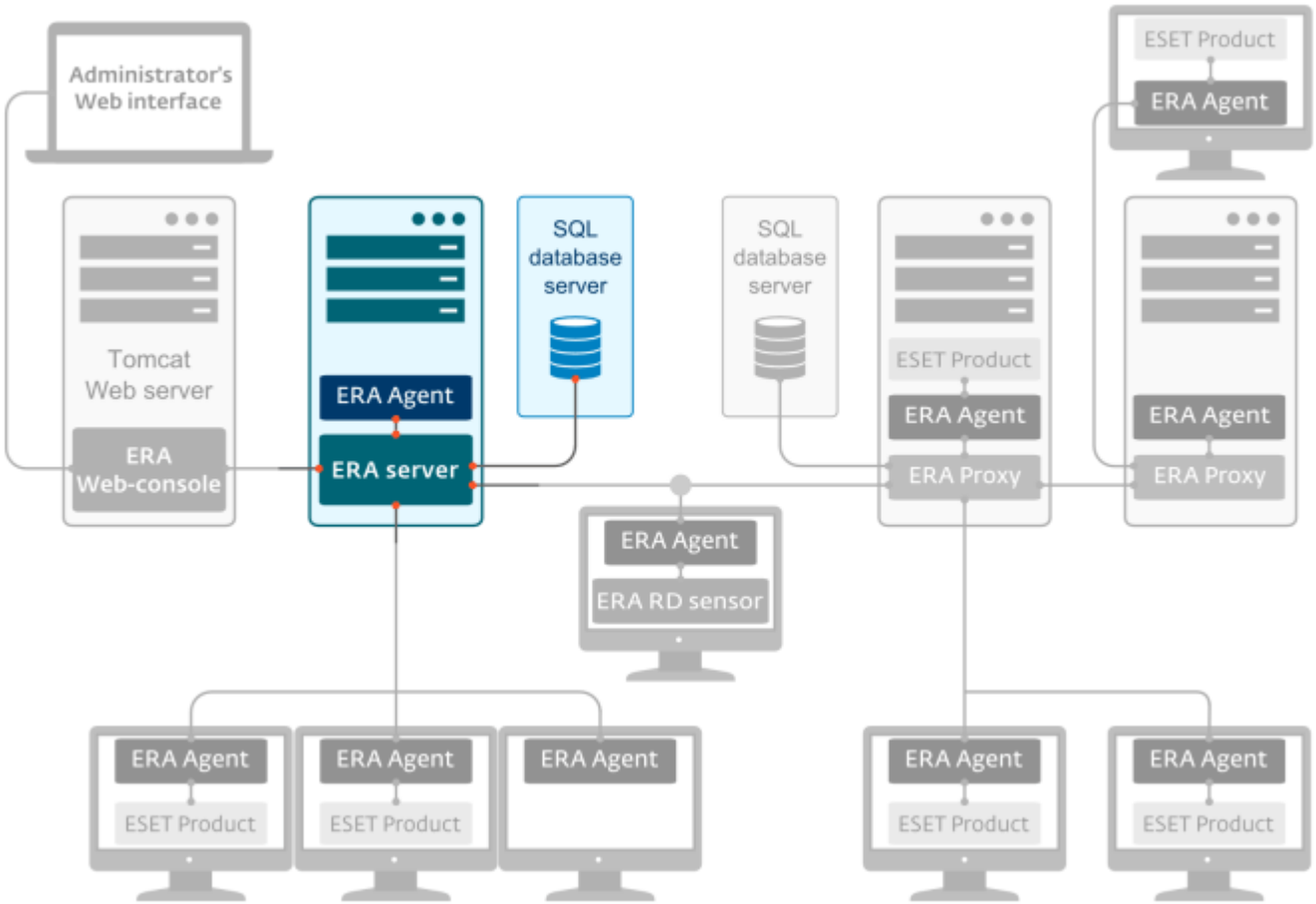
- Server ERA
- ERA Web Console
- Agente ERA

I seguenti componenti di supporto sono facoltativi. Si consiglia di installarli per ottenere prestazioni ottimizzate dall'applicazione sulla rete:

- Proxy ERA
- Sensore RD
- Connettore dispositivi mobili
- Proxy Apache HTTP

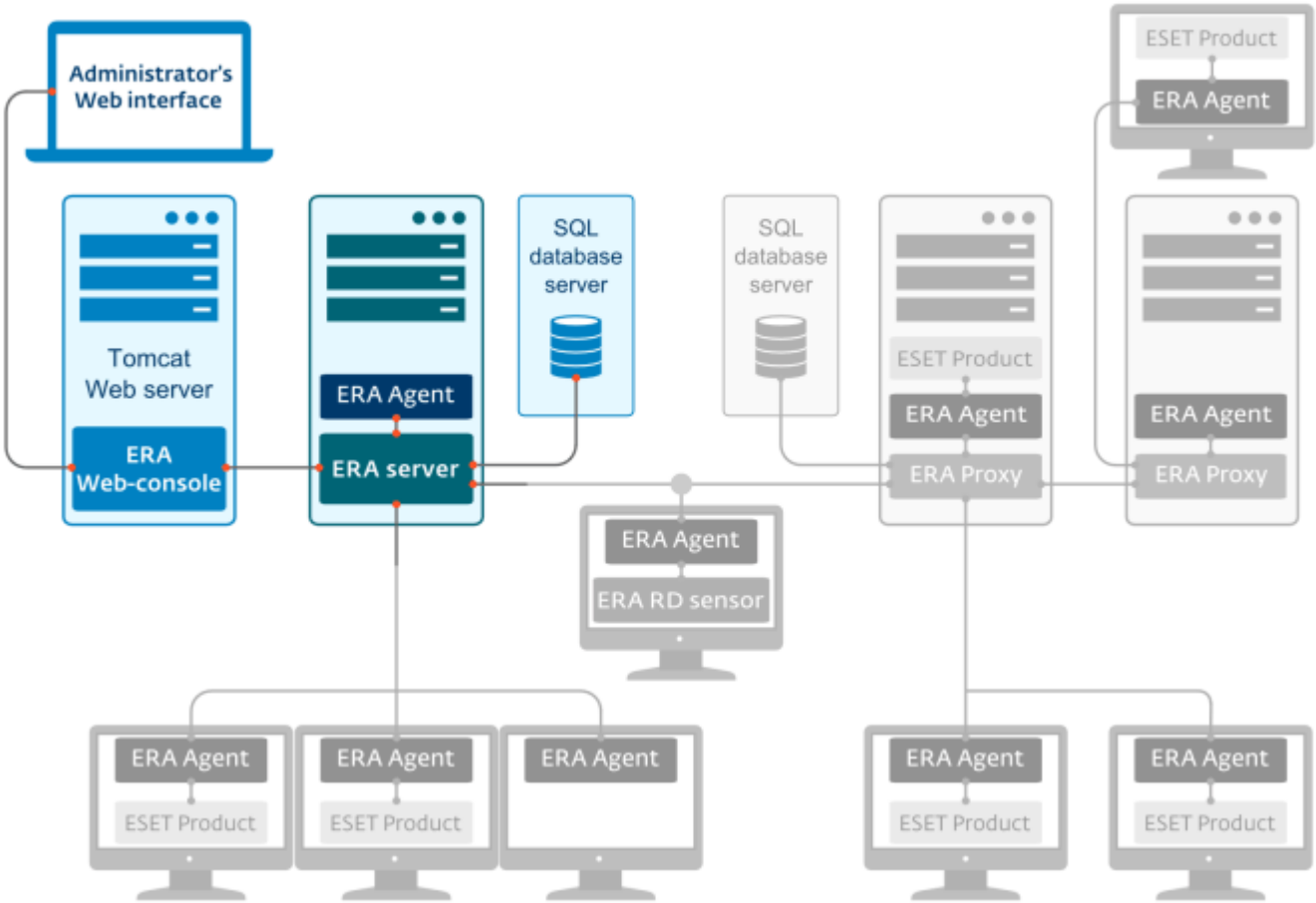
1.2.1 Server

ESET Remote Administrator Server è l'applicazione esecutiva che elabora tutti i dati ricevuti dai client che si connettono al server (attraverso l'Agente ERA). Per una corretta elaborazione dei dati, il server richiede una connessione stabile a un server del database sul quale sono archiviati i dati di rete. Per ottenere prestazioni ottimizzate, si consiglia di installare il server del database su un altro computer.



1.2.2 Console Web

ERA Web Console è un'interfaccia utente basata sul Web che consente all'utente di gestire soluzioni di protezione ESET nell'ambiente di lavoro, di visualizzare una panoramica dello stato dei client sulla rete e di utilizzare da remoto soluzioni ESET su computer non gestiti. L'accesso alla console Web viene effettuato tramite il browser (vedere Browser Web supportati). Se si decide di rendere il server Web accessibile da Internet, è possibile utilizzare ESET Remote Administrator praticamente da qualsiasi posizione e dispositivo.



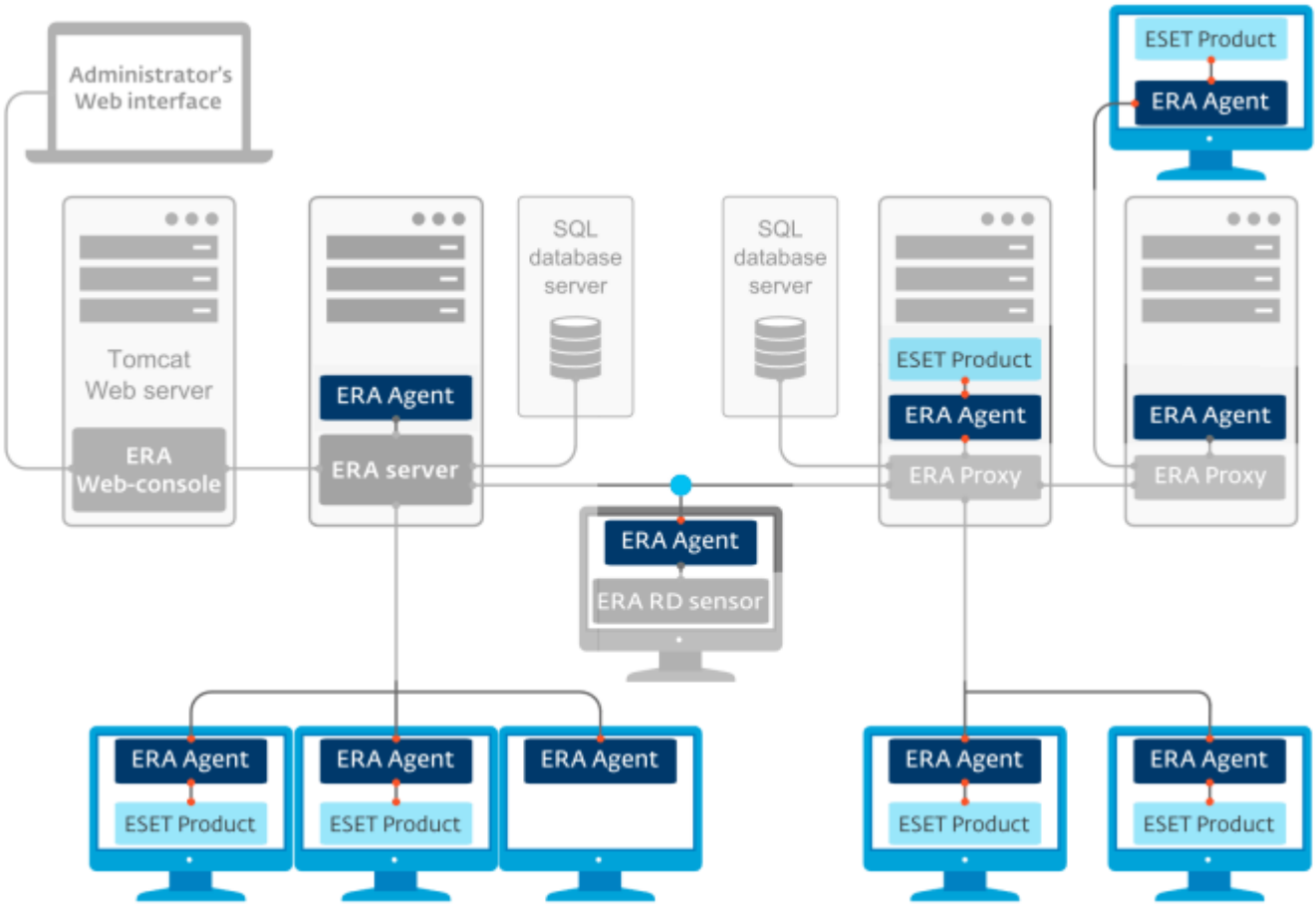
1.2.3 Agente

L'agente rappresenta un componente essenziale di ESET Remote Administrator. I client non comunicano direttamente con il server, ma è l'agente a facilitare la comunicazione. L'agente raccoglie informazioni dal client e le invia al server ERA. Se il server ERA invia un'attività per il client, ciò significa che l'attività viene inviata all'agente che provvede poi a inviarla al client.

Per semplificare l'implementazione della protezione dell'endpoint, nella suite ERA è incluso l'agente ERA indipendente (a partire dalla versione 6). Si tratta di un servizio semplice, altamente modulare e leggero che copre tutte le comunicazioni tra il server ERA e qualsiasi prodotto ESET o sistema operativo. Anziché comunicare direttamente con il server ERA, i prodotti ESET comunicano attraverso l'agente. I computer client sui quali è installato l'agente ESET e che comunicano con il server ERA sono considerati "gestiti". È possibile installare l'agente su qualsiasi computer indipendentemente dal fatto che siano stati installati altri software ESET.

I vantaggi sono:

- Configurazione semplice: è possibile distribuire l'agente nell'ambito di un'installazione aziendale standard.
- Gestione della protezione in loco: poiché l'agente viene configurato in modo da memorizzare vari scenari di protezione, i tempi di reazione alle minacce vengono ridotti drasticamente.
- Gestione della protezione off-line: l'agente risponde a un evento se non è connesso al server ERA.



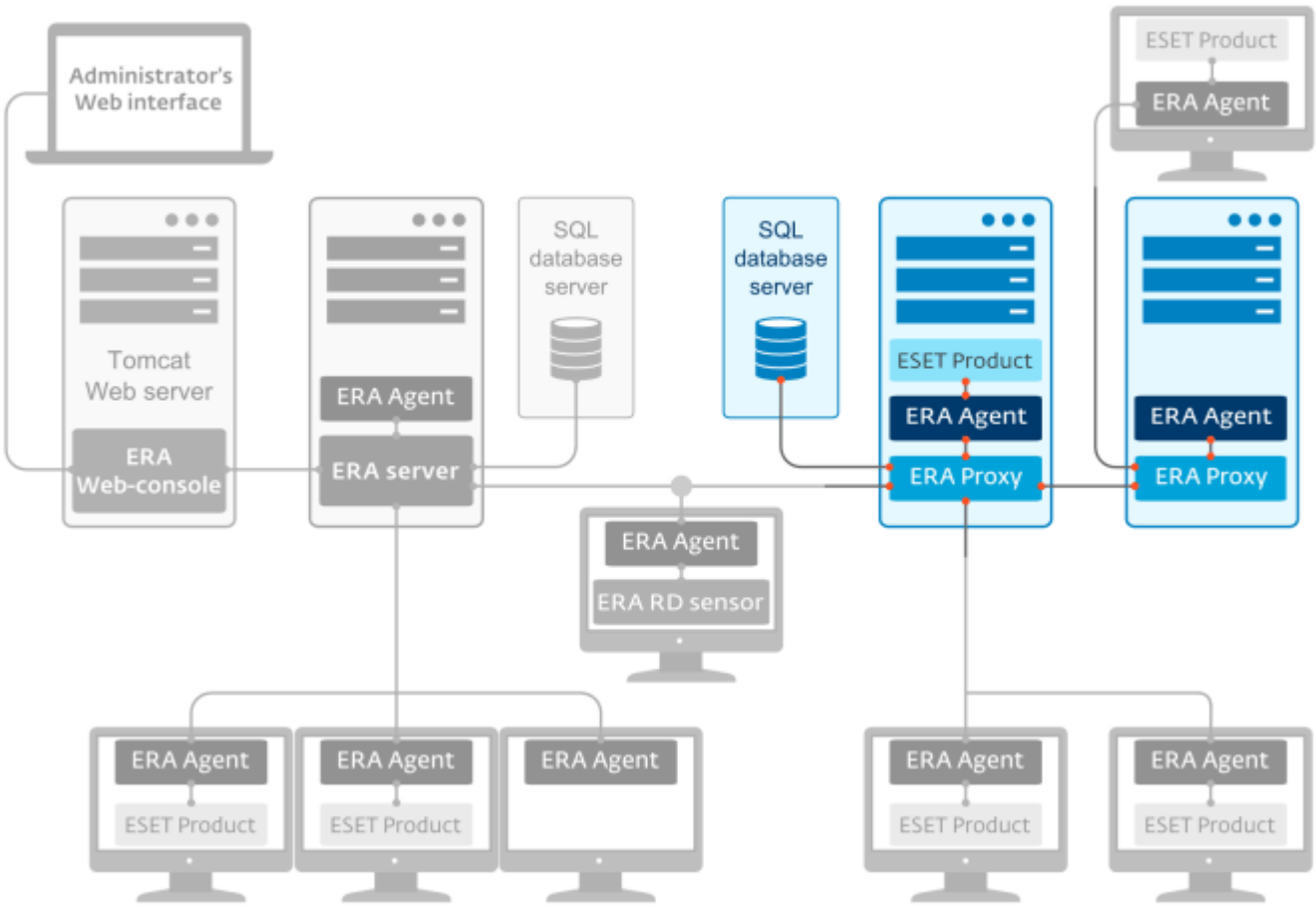
1.2.4 Proxy

Il server del **Proxy ERA** è una versione leggera del componente server. Questo tipo di server viene utilizzato per garantire un elevato livello di scalabilità. Il server del proxy ERA consente all'utente di concentrare il traffico proveniente dagli agenti client. e ad agenti multipli di connettersi al proxy ERA che distribuirà il traffico al server ERA. Ciò consente di ottimizzare le query relative al database. Il proxy ERA è anche in grado di connettersi ad altri server proxy e successivamente al server ERA. Tutto dipende dall'ambiente di rete e dalla relativa configurazione.

Il proxy ERA è anche responsabile della distribuzione passiva dei dati di configurazione (gruppi, criteri, attività, ecc.) agli agenti. L'inoltro non implica il coinvolgimento del server ERA.

L'unico modo per configurare il proxy ERA (e tutti gli altri componenti) è rappresentato dal criterio inviato dal server ERA. Ciò significa che è necessario installare l'agente sulla macchina del proxy ERA per inviare la configurazione dal server ERA al componente del proxy ERA.

NOTA: il server ERA non può connettersi direttamente al server del proxy ERA in assenza dell'agente.



Il **Proxy ERA** è un altro componente di ESET Remote Administrator che consente di soddisfare due requisiti. In caso di reti di medie dimensioni o aziendali caratterizzate dalla presenza di numerosi client (ad esempio, 10.000 client o più), è possibile utilizzare il proxy ERA per distribuire il carico tra molteplici proxy ERA, allo scopo di non sovraccaricare il Server ERA principale. Un altro vantaggio del proxy ERA consiste nella possibilità di utilizzarlo per connettersi a una filiale aziendale da remoto con un collegamento debole. Ciò significa che l'agente ERA su ciascun client non si connette direttamente al server ERA principale ma attraverso il proxy ERA, che si trova sulla stessa rete locale della filiale aziendale. Questo tipo di configurazione offre comunicazioni ottimizzate con la filiale aziendale. Il proxy ERA accetta connessioni da tutti gli agenti ERA locali, ne compila i dati e li carica sul server ERA principale (o un altro proxy ERA). Tale operazione consente alla rete di adattare altri client senza compromettere le proprie prestazioni e la qualità delle query relative al database.

Per un corretto funzionamento del proxy ERA, il computer host sul quale è stato installato il proxy ERA deve prevedere un agente ESET installato ed essere connesso al livello superiore (l'eventuale server ERA o un proxy ERA superiore) della rete in uso.

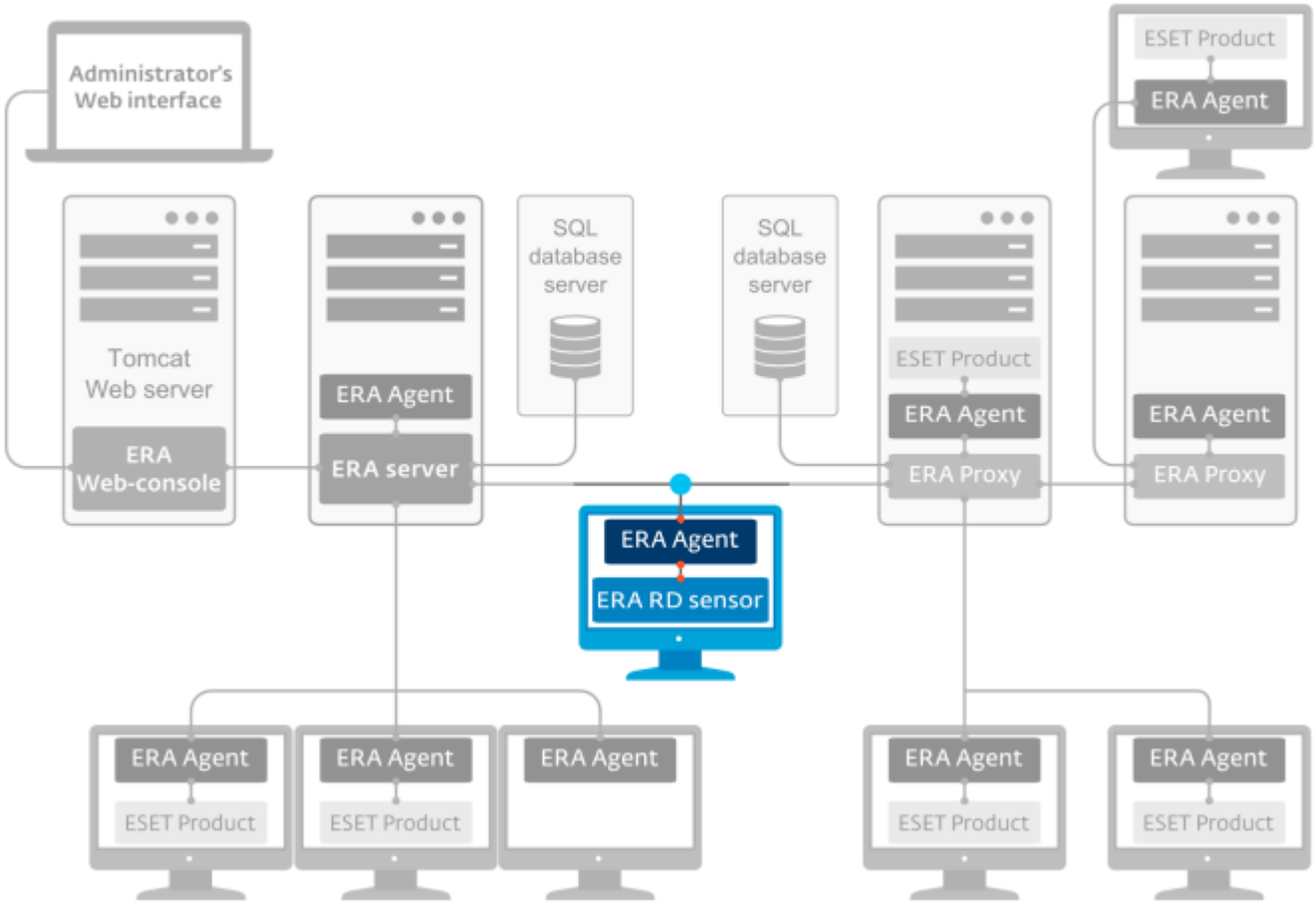
NOTA: Osservare lo scenario di distribuzione con il Proxy ERA.

1.2.5 Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) è uno strumento di rilevamento di sistema rogue che consente di ricercare computer nella rete in uso. L'utilità del sensore consiste nella sua capacità di individuare nuovi computer da ESET Remote Administrator risparmiando all'utente il compito di ricercarli e aggiungerli manualmente. Le macchine rilevate vengono immediatamente localizzate e segnalate in un report predefinito, consentendo in tal modo all'utente di spostarle in gruppi statici specifici e di procedere con le attività di gestione.

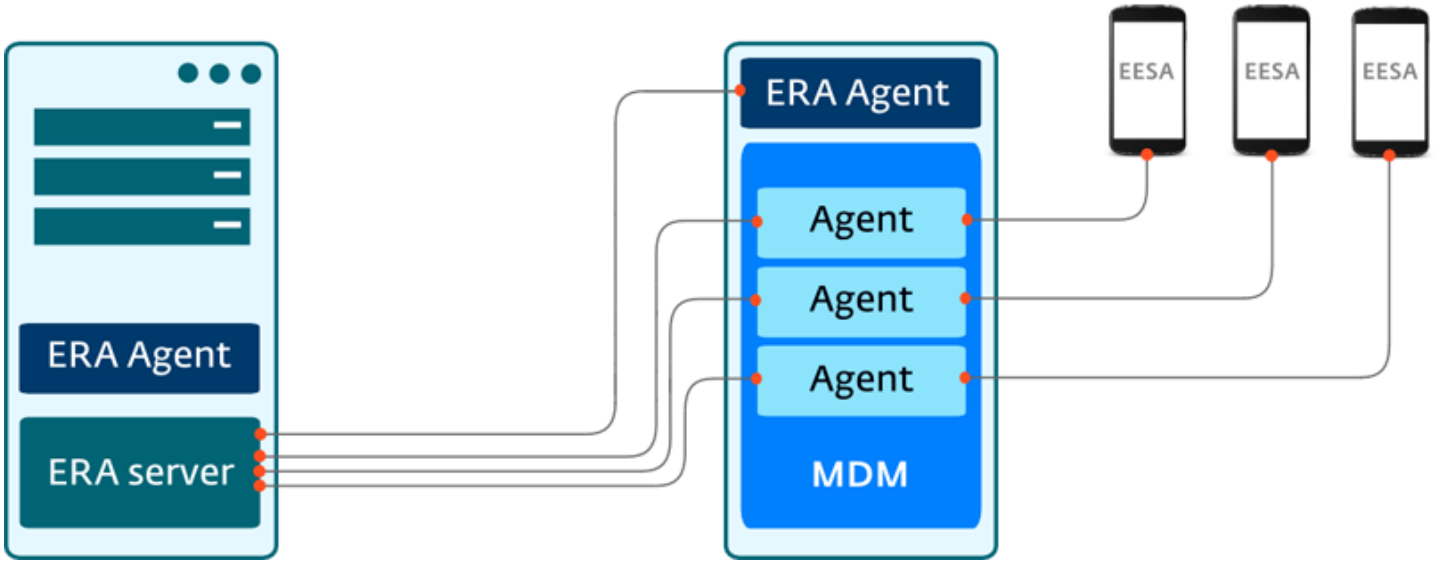
RD Sensor è un ascoltatore passivo che rileva i computer presenti nella rete e invia le relative informazioni al server ERA. A questo punto, il server ERA valuta se i PC trovati nella rete sono sconosciuti o già gestiti.

Ogni computer all'interno della struttura di rete (dominio, LDAP, rete Windows) viene aggiunto automaticamente all'elenco di computer del server ERA attraverso un'attività di sincronizzazione del server. RD Sensor è un metodo utile per ricercare computer non presenti nel dominio o in un'altra struttura di rete e aggiungerli al server ESET Remote Administrator. RD Sensor è in grado di ricordare i computer che sono già stati rilevati evitando in tal modo di inviare le stesse informazioni due volte.



1.2.6 Connettore dispositivi mobili

Connettore dispositivi mobili è un'applicazione che consente all'utente di gestire dispositivi mobili e amministrare ESET Endpoint Security for Android.



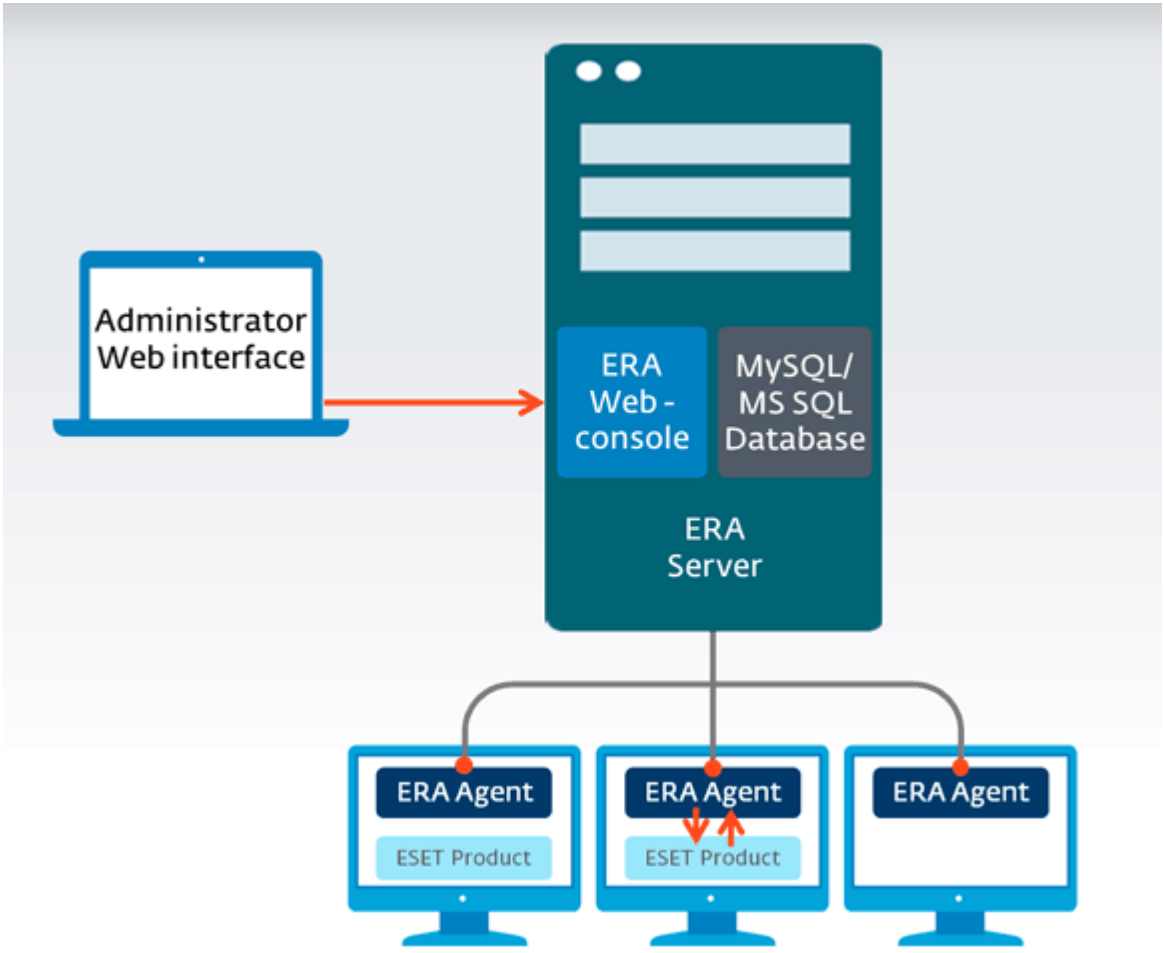
1.2.7 Scenari di utilizzo

Nei capitoli che seguono, verranno analizzati scenari di utilizzo per diversi ambienti di rete. Per istruzioni più dettagliate, consultare il capitolo appropriato:

- Server singolo (aziende di piccole dimensioni)
- Alta disponibilità (Enterprise)
- Diramazioni remote con proxy

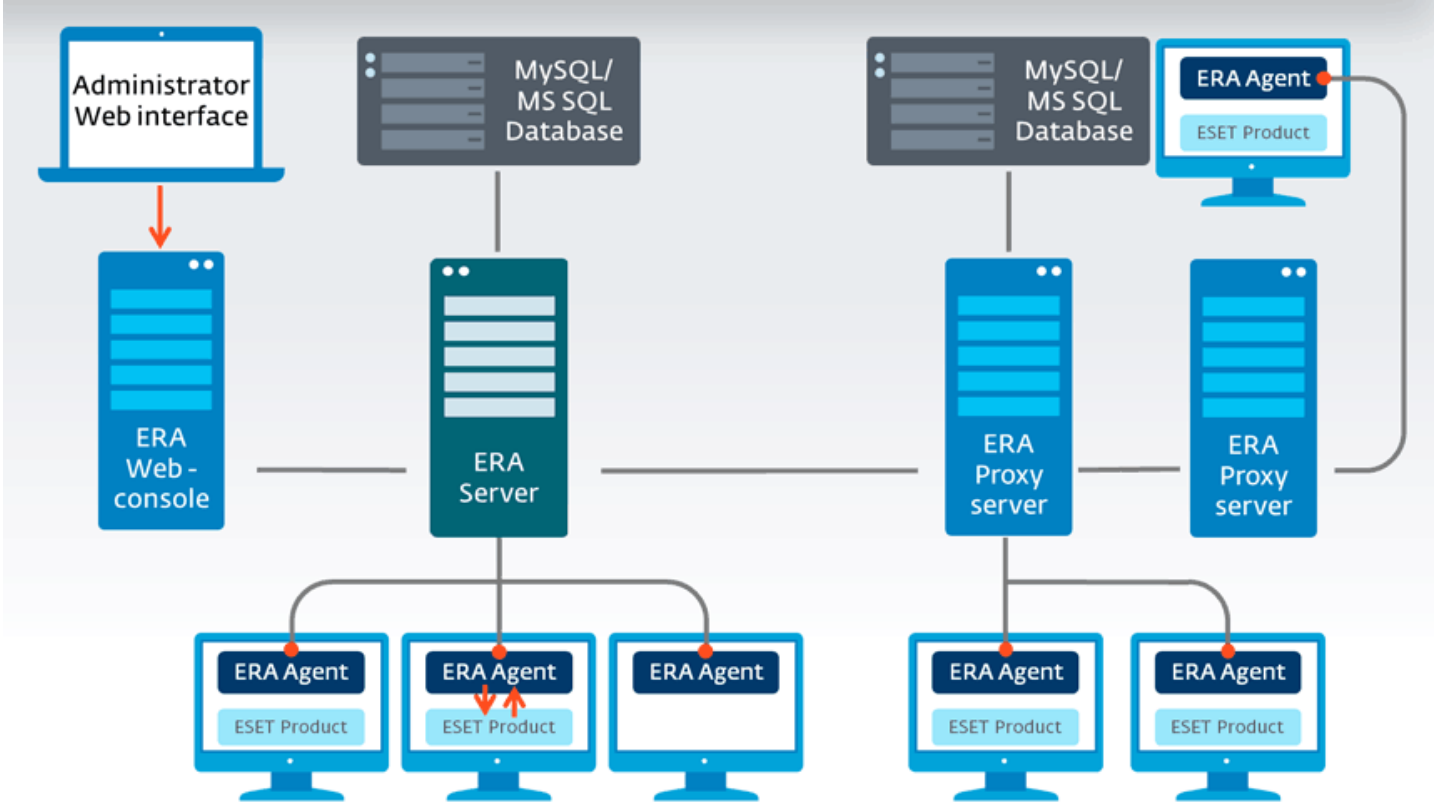
1.2.7.1 Server singolo (aziende di piccole dimensioni)

Per gestire reti di piccole dimensioni (massimo 1000 client), è sufficiente disporre solitamente di un'unica macchina su cui sono installati il server ERA e i relativi componenti (server Web fornito, database, ecc.). È possibile immaginarlo come un server singolo o un'installazione indipendente. Tutti i client gestiti sono connessi direttamente al server ERA attraverso l'agente ERA. L'amministratore si connette a ERA Web Console attraverso il browser Web da qualsiasi computer presente nella rete oppure esegue la console Web direttamente dal server ERA.



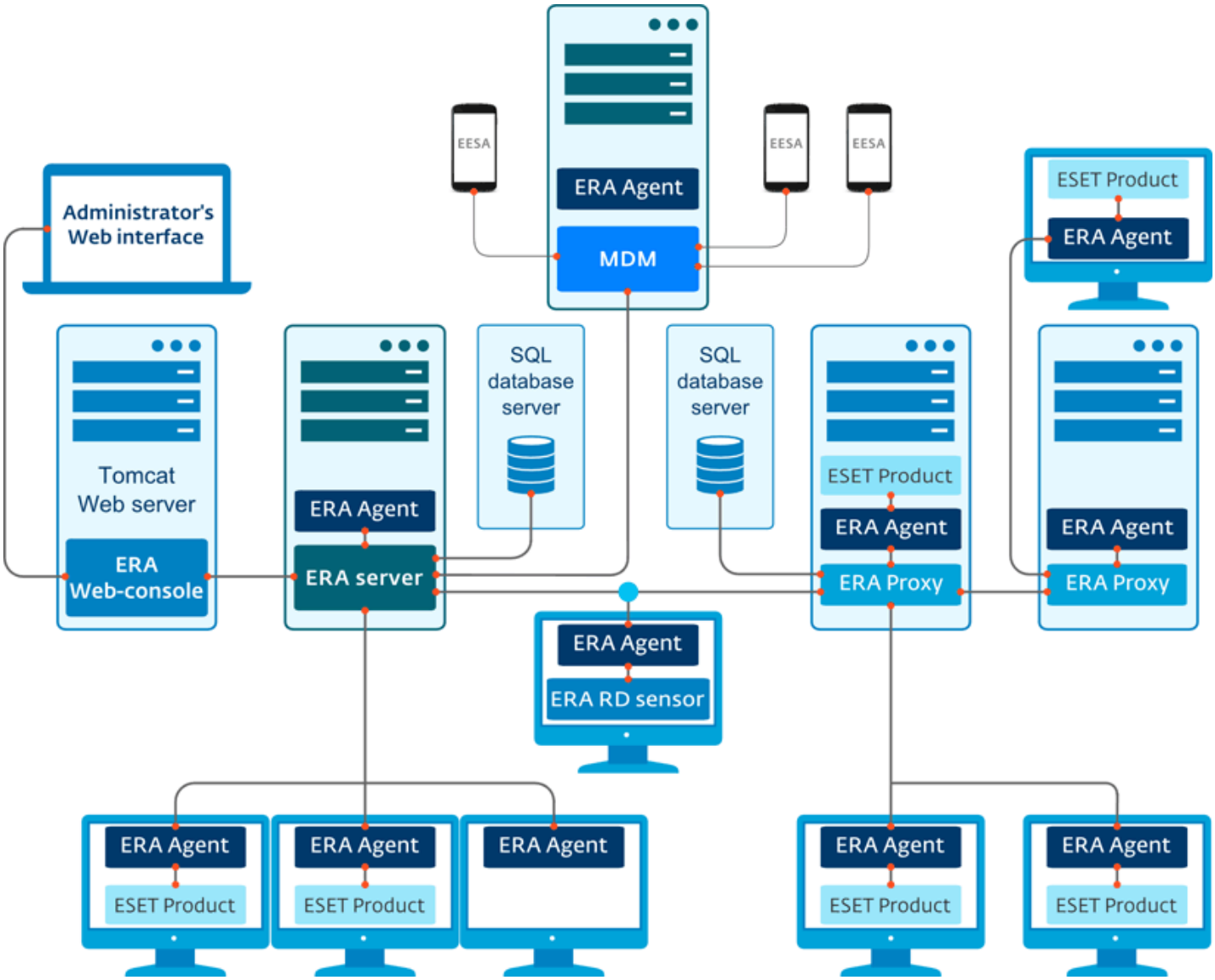
1.2.7.2 Diramazioni remote con proxy

In una rete di medie dimensioni (formata, ad esempio, da 10.000 client), viene aggiunto un altro livello formato da server del proxy ERA. Gli agenti ERA sono connessi al server del proxy ERA, che viene aggiunto a causa della presenza di un collegamento debole al sito remoto (ad esempio, una filiale aziendale). Tuttavia, è sempre possibile collegare gli agenti ERA (collocati su un sito remoto) direttamente al server principale.



1.2.7.3 Alta disponibilità (Enterprise)

Per gli ambienti Enterprise (formati, ad esempio, da 100.000 client), è necessario utilizzare componenti ERA aggiuntivi. Uno è l'RD Sensor, che aiuta l'utente a ricercare nuovi computer nella rete. L'altro è un livello dei server del proxy ERA. Gli agenti ERA sono collegati al server del proxy ERA e bilanciano, in tal modo, il carico sul server principale che rappresenta una risorsa importante per le prestazioni del sistema. È sempre possibile utilizzare questa configurazione per collegare gli agenti ERA direttamente al server principale. Per garantire ridondanza, viene inoltre implementato un database SQL su un cluster di failover.



1.2.8 Esempi di utilizzi pratici

Per ottenere prestazioni ottimizzate, si consiglia di utilizzare Microsoft SQL Server come database ESET Remote Administrator. Mentre ESET Remote Administrator è compatibile con MySQL, l'utilizzo di MySQL può influire negativamente sulle prestazioni del sistema in caso di gestione di grandi quantità di dati, tra cui dashboard, minacce e client. Lo stesso hardware con Microsoft SQL Server è in grado di gestire all'incirca 10 volte il numero di client rispetto a MySQL.

Per scopi di testing, ciascun client archivia circa 30 rapporti nel database. Microsoft SQL Server utilizza grandi porzioni di RAM per la cache dei dati del database. Si consiglia pertanto di verificare che sia presente una quantità di memoria corrispondente almeno a quella presente sul disco di Microsoft SQL Server.

Non è facile calcolare il numero esatto di risorse utilizzate da ESET Remote Administrator, in quanto queste variano in base alla configurazione di rete del sistema. Seguono i risultati dei test relativi a configurazioni di rete comuni:

- Esempio di test: massimo 5.000 client che si connettono a ERA Server
- Esempio di test: massimo 100.000 client che si connettono al server ERA

Per ottenere una configurazione ottimale, in grado di soddisfare le esigenze dell'utente, si consiglia di eseguire il test su un numero inferiore di client e un hardware più lento e di elaborare i requisiti di sistema sulla base dei risultati del test.

ESEMPIO DI TEST (5.000 CLIENT)

Hardware/software

- Windows Server 2003 R2, architettura processore x86
- Microsoft SQL Server Express 2008 R2
- Intel Core2Duo E8400 @3 GHz
- 3 GB di RAM
- Seagate Barracuda 7200 rpm, 500 GB, cache 16 MB, Sata 3,0 GB/s

Risultati

- ERA Web Console è molto reattiva (meno di 5 s)
- Consumo memoria:
  - Apache Tomcat 200 MB
  - ERA Server 200 MB
  - SQL Server Database 1 GB
- Prestazioni replica server: 10 repliche al secondo
- Dimensione database su disco: 1 GB (5.000 client, ciascuno con 30 rapporti nel database)

Per questo esempio, è stato utilizzato SQL Server Express 2008 R2. Nonostante i limiti (database 10 GB, 1 CPU e utilizzo di 1 GB di RAM), questa configurazione era funzionale e ha registrato buone prestazioni. L'utilizzo di SQL Server Express è consigliato per i server contenenti meno di 5.000 client. È possibile utilizzare inizialmente SQL Server Express ed effettuare l'aggiornamento a Microsoft SQL Server (versione completa) qualora diventi necessario utilizzare un database di maggiori dimensioni. Tenere presente che le versioni precedenti di Express (<2008 R2) presentano un limite di 4 GB per il database su disco.

Le prestazioni relative alle repliche del server definiscono un intervallo di repliche per i client. 10 repliche al secondo si traducono in 600 repliche al minuto. Di conseguenza, in un caso ideale, l'intervallo di replica su tutti i 5.000 client dovrebbe essere impostato su 8 minuti. Tale parametro determinerebbe però un carico del 100% sul server. In tal caso, è necessario pertanto impostare un intervallo più lungo. In questo esempio, si raccomanda un intervallo di replica di 20-30 minuti.

ESEMPIO DI TEST (100.000 CLIENT)

Hardware/software

- Windows Server 2012 R2 Datacenter, architettura processore x64
- Microsoft SQL Server 2012
- Intel Xeon E5-2650v2 @2.60 GHz
- 64 GB di RAM
- Adattatore di rete Intel NIC/PRO/1000 PT Dual
- 2x Micron RealSSD C400 Unità SSD 256 GB (una per sistema + software, la seconda per i file dati SQL Server)

Risultati

- La console Web è reattiva (meno di 30 s)
- Consumo memoria
  - Apache Tomcat 1 GB
  - ERA Server 2 GB
  - SQL Server Database 10 GB
- Prestazioni replica server: 80 repliche al secondo
- Dimensione database su disco: 10 GB (100.000 client, ciascuno con 30 rapporti nel database)

In questo caso, è stato scelto di installare tutti i componenti (Apache Tomcat + console Web, ERA Server, SQL Server) su una macchina per testare la capacità di ERA Server.

Il numero elevato di client ha determinato un aumento dell'utilizzo della memoria e del disco da parte di Microsoft SQL Server. Per ottenere prestazioni ottimali, SQL Server memorizza nella cache quasi tutti i dati del database archiviato nella memoria. Anche Apache Tomcat (console Web) ed ERA memorizzano i dati nella cache e ciò spiega l'aumento dell'utilizzo di memoria in questo esempio.

ERA Server è in grado di servire 80 repliche al secondo (288.000 all'ora). Di conseguenza, in una situazione ideale, l'intervallo di replica su tutti i 100.000 client dovrebbe essere impostato su "ogni ~30 minuti" (carico di 200.000 repliche all'ora), ma ciò condurrebbe a un carico del server del 100%. L'intervallo di replica migliore è pertanto di 1 ora (100.000 repliche all'ora).

L'utilizzo dei dati di rete dipende dal numero di rapporti raccolti dai client. In questo caso, il numero corrispondeva a circa 20 KB a replica, di conseguenza 80 repliche al secondo generano una velocità di rete di circa 1600 KB/s (20 Mbit/s).

In questo esempio, è stato utilizzato uno scenario basato su un server singolo. Il carico di CPU e di rete verrà distribuito in modo ottimale in caso di utilizzo di più di un proxy ERA (maggiore è il numero migliori saranno le prestazioni). Tale situazione determinerà una distribuzione del carico sia di CPU sia di rete durante le repliche dei client. È buona norma distribuire il carico di rete, specialmente nel caso di client distanti tra di loro. L'intervallo di replica del proxy sul server può essere eseguito durante le ore di mancato utilizzo del sistema, quando la velocità della rete dalle posizioni distanti è migliore.

1.3 Prodotti e lingue supportati

ESET Remote Administrator consente all'utente di distribuire, attivare o gestire i seguenti prodotti ESET:

Gestibile tramite ESET Remote Administrator 6	Versione prodotto	Metodo di attivazione
ESET Endpoint Security per Windows	6.x e 5.x	6.x: chiave di licenza 5.x: nome utente/password
ESET Endpoint Antivirus per Windows	6.x e 5.x	6.x: chiave di licenza 5.x: nome utente/password
ESET Endpoint Security per OS X	6.x	Chiave di licenza
ESET Endpoint Antivirus per OS X	6.x	Chiave di licenza
ESET Endpoint Security per Android	2.x	Chiave di licenza

Gestibile tramite ESET Remote Administrator 6	Versione prodotto	Metodo di attivazione
ESET File Security per Windows Server	6.x	Chiave di licenza
ESET File Security per Microsoft Windows Server	4.5.x	Nome utente/password
ESET NOD32 Antivirus 4 Business Edition per Mac OS X	4.x	Nome utente/password
ESET NOD32 Antivirus 4 Business Edition per Linux Desktop	4.x	Nome utente/password
ESET Mail Security per Microsoft Exchange Server	4.5.x	Nome utente/password
ESET Mail Security per IBM Lotus Domino	4.5.x	Nome utente/password
ESET Security per Microsoft Windows Server Core	4.5.x	Nome utente/password
ESET Security per Microsoft SharePoint Server	4.5.x	Nome utente/password
ESET Security per Kerio	4.5.x	Nome utente/password
ESET NOD32 Antivirus Business Edition	4.2.76	Nome utente/password
ESET Smart Security Business Edition	4.2.76	Nome utente/password

NOTA: Le versioni dei prodotti Windows Server precedenti a quelle visualizzate nella tabella indicata in precedenza non possono al momento essere gestite utilizzando ESET Remote Administrator.

Lingue supportate

Nome	Codice
Inglese (Stati Uniti)	en-US
Arabo (Egitto)	ar-EG
Cinese semplificato	zh-CN
Cinese tradizionale	zh-TW
Croato (Croazia)	hr-HR
Ceco (Repubblica Ceca)	cs-CZ
Francese (Francia)	fr-FR
Francese (Canada)	fr-FC
Tedesco (Germania)	de-DE
Italiano (Italia)	it-IT
Giapponese (Giappone)	ja-JP
Coreano (Corea)	ko-KR
Polacco (Polonia)	pl-PL
Portoghese (Brasile)	pt-BR
Russo (Russia)	ru-RU
Spagnolo (Cile)	es-CL
Spagnolo (Spagna)	es-ES
Slovacchia (Slovacchia)	sk-SK

2. Requisiti di sistema

È disponibile un set di prerequisiti relativi a hardware, database e software che è necessario soddisfare per installare ESET Remote Administrator.

2.1 Hardware

Per il corretto funzionamento di ESET Remote Administrator, il sistema deve soddisfare i seguenti requisiti hardware:

Memoria	4 GB di RAM
Disco rigido	Almeno 20 GB di spazio libero
Processore	Dual-Core, 2,0 GHz o superiore
Connessione di rete	1 Gbit/s

2.2 Database

ESET Remote Administrator supporta due tipi di server di database:

- Microsoft SQL Server (incluse le edizioni Express e non-Express) 2008, 2008 R2, 2012, 2014
- MySQL (versione 5.5 e successive)

È possibile specificare il server del database che si desidera utilizzare durante l'installazione del Server o del Proxy. Microsoft SQL Server 2008 R2 Express viene installato per impostazione predefinita e fa parte del pacchetto di installazione. Si tenga presente che Microsoft SQL Server 2008 R2 Express prevede un limite di 10 GB per il database e non può essere installato su un controller di dominio, ad esempio, se si utilizza Microsoft SBS, si consiglia di installare ESET Remote Administrator su un server diverso o di non selezionare il componente SQL Server Express durante l'installazione (tale operazione richiede l'utilizzo della versione di SQL o MySQL Server esistente per l'esecuzione del database ERA).

Se si decide di utilizzare Microsoft SQL Server, la versione più recente supportata è **Microsoft SQL Server 2008**. È possibile utilizzare un Microsoft SQL Server esistente in esecuzione nell'ambiente di lavoro. Tuttavia, è necessario che vengano soddisfatti alcuni requisiti minimi.

NOTA: il server ERA e il proxy ERA non utilizzano un backup integrato. Di conseguenza, si consiglia vivamente di effettuare il backup del server del database al fine di prevenire la perdita di dati.

Requisiti hardware del server del database:

Memoria	1 GB di RAM
Disco rigido	Almeno 10 GB di spazio libero
Velocità processore	Processore x86: 1,0 GHz Processore x64: 1,4 GHz **Nota**: per ottenere prestazioni ottimali, si consiglia di utilizzare un processore con una potenza minima di 2,0 GHz.
Tipo di processore	Processore x86: Processore compatibile con Pentium III o superiore Processore x64: AMD Opteron, AMD Athlon 64, Intel Xeon con supporto Intel EM64T, Intel Pentium IV con supporto EM64T

2.3 Sistemi operativi supportati

Le sezioni che seguono illustrano le versioni dei sistemi operativi supportate in Windows, Linux e Mac OS da uno specifico componente di ESET Remote Administrator.

2.3.1 Windows

La tabella che segue consente di visualizzare un elenco di sistemi operativi supportati per ciascun componente di ESET Remote Administrator. È inoltre possibile installare il server ERA, il proxy ERA e l'MDM su un sistema operativo client (*Microsoft Windows 7, 8, 8.1) **solo per scopi di valutazione**.

Sistema operativo	Server	Agente	Proxy	RD Sensor	MDM
Windows XP x86 SP3		X		X	
Windows XP x64 SP2		X		X	
Windows Vista x86 SP2		X		X	
Windows Vista x64 SP2		X		X	
Windows 7 x86 SP1	*	X	*	X	*
Windows 7 x64 SP1	*	X	*	X	*
Windows 8 x86	*	X	*	X	*
Windows 8 x64	*	X	*	X	*
Windows 8.1 x86	*	X	*	X	*
Windows 8.1 x64	*	X	*	X	*
Windows HomeServer 2003 SP2		X		X	
Windows HomeServer 2011 x64		X		X	
Windows Server 2003 x86 SP2	X	X	X	X	
Windows Server 2003 x64 SP2	X	X	X	X	
Windows Server 2003 x86 R2 SP2	X	X	X	X	
Windows Server 2003 x64 R2 SP2	X	X	X	X	
Windows Server 2008 x64 R2 SP1	X	X	X	X	X
Windows Server 2008 x64 R2 CORE	X	X	X	X	X
Windows Server 2008 x86		X		X	
Windows Server 2008 x86 SP2	X	X	X	X	X
Windows Server 2008 x64		X		X	
Windows Server 2008 x64 SP2	X	X	X	X	X
Windows Server 2012 x64	X	X	X	X	X
Windows Server 2012 x64 CORE	X	X	X	X	X
Windows Server 2012 x64 R2	X	X	X	X	X
Windows Server 2012 x64 R2 CORE	X	X	X	X	X
Microsoft SBS 2003 x86 SP2 **	X	X	X	X	X
Microsoft SBS 2003 x86 R2 **	X	X	X	X	X
Microsoft SBS 2008 x64		X		X	
Microsoft SBS 2008 x64 SP2 **	X	X	X	X	X
Microsoft SBS 2011 x64 Standard	X	X	X	X	X
Microsoft SBS 2011 x64 Essential	X	X	X	X	X

*** Componenti ERA in esecuzione sui sistemi operativi client (solo per scopi di valutazione).**

**** Microsoft SQL Server Express incluso in Microsoft Small Business Server (SBS) non è supportato da ESET Remote Administrator**. Se si desidera eseguire il database ERA su SBS, è necessario utilizzare una versione più recente di Microsoft SQL Server. Per ulteriori informazioni e istruzioni, consultare Installazione su Windows SBS/Essentials**.**

Sulle versioni precedenti dei sistemi operativi, ad esempio Windows Server 2003, la crittografia dei protocolli potrebbe non essere completamente supportata sul lato del sistema operativo. Di conseguenza, verrà utilizzato TLSv1.0 al posto di TLSv1.2, (TLSv1.0 è considerato meno sicuro rispetto alle versioni più recenti). Questa situazione si verifica anche nel momento in cui, a differenza del client, il sistema operativo supporta TLSv1.2. In tal caso, la comunicazione si verifica mediante TLS1.0. Se si desiderano comunicazioni più sicure, si suggerisce di utilizzare sistemi operativi e client più recenti (Windows Server 2008 R2 e versioni successive dei server e Windows Vista e versioni successive dei client).

NOTA: È possibile installare su un sistema operativo desktop ed effettuare la distribuzione degli accessori virtuali. In questo modo è possibile eseguire ESET Remote Administrator su un sistema operativo non server senza la necessità di utilizzare ESXi.

2.3.2 Linux

Sistema operativo	Server	Agente	Proxy	RD Sensor	MDM
Ubuntu 12.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x86 Server	X	X	X	X	X
Ubuntu 12.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x64 Server	X	X	X	X	X
Ubuntu 14.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x86 Server	X	X	X	X	X
Ubuntu 14.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x64 Server	X	X	X	X	X
RHEL 5 x86		X			
RHEL 5 x64		X			
RHEL Server 6 x86	X	X	X	X	X
RHEL Server 6 x64	X	X	X	X	X
RHEL Server 7 x86	X	X	X	X	X
RHEL Server 7 x64	X	X	X	X	X
CentOS 5 x86		X			
CentOS 5 x64		X			
CentOS 6 x86	X	X	X	X	X
CentOS 6 x64	X	X	X	X	X
CentOS 7 x86	X	X	X	X	X
CentOS 7 x64	X	X	X	X	X
SLED 11 x86	X	X	X	X	X
SLED 11 x64	X	X	X	X	X
SLES 11 x86	X	X	X	X	X
SLES 11 x64	X	X	X	X	X
OpenSUSE 13 x86	X	X	X	X	X
OpenSUSE 13 x64	X	X	X	X	X
Debian 7 x86	X	X	X	X	X
Debian 7 x64	X	X	X	X	X
Fedora 19 x86	X	X	X	X	X
Fedora 19 x64	X	X	X	X	X
Fedora 20 x86	X	X	X	X	X
Fedora 20 x64	X	X	X	X	X

2.3.3 OS X

Sistema operativo	Agente
OS X 10.7 Lion	X
OS X 10.8 Mountain Lion	X
OS X 10.9 Mavericks	X
OS X 10.10 Yosemite	X

NOTA: OS X è supportato solo come client. Non è possibile installare ERA Server su OS X.

2.4 Porte utilizzate

Nei seguenti grafici vengono riportate tutte le possibili porte di comunicazione sulla rete utilizzate quando ESET Remote Administrator e i relativi componenti sono installati sull'infrastruttura. Altre comunicazioni vengono eseguite tramite i processi del sistema operativo nativo (ad esempio NetBIOS su TCP/IP).

Server ERA:

Protocollo	Porta	Utilizzo	Descrizioni
TCP	2222	ERA Server in ascolto	Comunicazione tra i client ed ERA Server
TCP	2223	ERA Server in ascolto	Comunicazione tra ERA Web Console ed ERA Server, utilizzata per l'installazione assistita
UDP	1237	Broadcast	Chiamata di riattivazione

ERA Web Console:

Protocollo	Porta	Utilizzo	Descrizioni
TCP	2223		Console Web
TCP	443		Console Web HTTP SSL

Proxy ERA:

Protocollo	Porta	Utilizzo	Descrizioni
TCP	3128		Proxy HTTP (caching di aggiornamento)
TCP	2222		Proxy

Agente ERA:

Protocollo	Porta	Utilizzo	Descrizioni
TCP	139	Porta di destinazione dal punto di vista di ERA Server	Utilizzo della condivisione ADMIN$
TCP	445	Porta di destinazione dal punto di vista di ERA Server	Accesso diretto alle risorse condivise tramite TCP/IP durante l'installazione remota (un'alternativa a TCP 139)
UDP	137	Porta di destinazione dal punto di vista di ERA Server	Risoluzione dei nomi durante l'installazione remota
UDP	138	Porta di destinazione dal punto di vista di ERA Server	Ricerca durante l'installazione remota

Connettore dispositivi mobili:

Protocollo	Porta	Utilizzo	Descrizioni
TCP	9980	Registrazione dispositivo mobile	Porta registrazione
TCP	9981	Comunicazione con ERA	Connettore dispositivi mobili si connette al server ERA

Le porte predefinite 2222, 2223 possono essere modificate se già in uso da parte di altre applicazioni.

NOTA: tutte le precedenti porte non devono essere utilizzate da altre applicazioni. In caso contrario, potrebbero verificarsi dei problemi.

NOTA: configurare il/i firewall nella rete in modo da consentire la comunicazione tramite le porte indicate sopra.

3. Processo di installazione

L'installazione di ESET Remote Administrator può essere eseguita in vari modi. Scegliere il tipo di installazione che si adatta maggiormente alle proprie esigenze e all'ambiente di lavoro. Il metodo più semplice, ovvero il programma di installazione ESET Remote Administrator (ERA) (installazione del pacchetto integrato), consente all'utente di installare ESET Remote Administrator e i relativi componenti su una sola macchina. L'installazione dei componenti consente di installare diversi componenti di ESET Remote Administrator su varie macchine. Ciò conferisce all'utente una maggiore libertà di personalizzazione dell'installazione. È possibile, infatti, installare ciascun componente su qualsiasi macchina, a condizione che vengano soddisfatti i requisiti di sistema. Per gli utenti che desiderano eseguire ERA in un ambiente virtualizzato, è disponibile la distribuzione su Accessori virtuali.

I programmi di installazione di ESET Remote Administrator sono disponibili in punti diversi. Ad esempio, nella sezione Download del sito Web di ESET sotto a **Gestione remota** (fare clic sul simbolo + per espandere la categoria). Da qui, è possibile scaricare i seguenti elementi:

- Pacchetto di installazione di ERA in formato compresso
- Programmi di installazione separati per ciascun componente
- Accessori virtuali (file OVA)
- Un'immagine ISO contenente tutti i programmi di installazione di ESET Remote Administrator (inclusi quelli elencati in precedenza)

Per installare ESET Remote Administrator, adottare la procedura che segue:

1. Assicurarsi che vengano soddisfatti tutti i Requisiti.
2. Scegliere Installazione del pacchetto (programma di installazione ERA integrato) oppure Installazione dei componenti sul sistema operativo Windows o Linux. In alternativa, è possibile utilizzare gli Accessori virtuali distribuendo un file OVA.
3. Scaricare il programma di installazione appropriato, il pacchetto del programma di installazione o programmi di installazione separati per ciascun componente che si desidera installare. È inoltre possibile scaricare il file OVA degli accessori virtuali o un'immagine ISO contenente tutti i programmi di installazione di ESET Remote Administrator.
4. Eseguire l'installazione in base alle istruzioni fornite nei capitoli successivi.
5. Se necessario, installare componenti opzionali (Server del proxy ERA, RD Sensor, Connettore dispositivi mobili)

Una volta terminato il processo di installazione, è possibile effettuare la connessione al server ERA utilizzando ERA Web Console e seguendo i primi passi di configurazione per poter iniziare a utilizzare ESET Remote Administrator.

3.1 Installazione pacchetto

L'installazione del pacchetto di ERA (programma di installazione integrato) è disponibile solo per sistemi operativi Windows e rappresenta un metodo di installazione pratico di tutti i componenti ERA attraverso l'utilizzo di una semplice procedura di configurazione guidata. Durante l'esecuzione del pacchetto di installazione, saranno disponibili due opzioni:

- Installazione del server Remote Administrator
- Installazione del proxy Remote Administrator

Installazione del server Remote Administrator

Utilizzare le istruzioni sottostanti, guardare il video illustrativo della Knowledge Base o leggere l'articolo della Knowledge Base per consultare le istruzioni dettagliate per il completamento dell'installazione mediante l'utilizzo del programma di installazione integrato.

1. Fare doppio clic sul pacchetto di installazione per avviare l'installazione. Selezionare **Server Remote Administrator**.

NOTA: Se si desidera installare ERA in un ambiente di Cluster di failover, è richiesta un'installazione dei componenti.

2. Selezionare i componenti che si desidera installare. Se non si dispone di un server del database, è possibile installare Microsoft SQL Server 2008 R2 Express, incluso nel pacchetto di installazione. Si tenga presente che Microsoft SQL Server 2008 R2 Express presenta un limite di 10 GB per il database. È inoltre possibile installare ERA Web Console, il Mobile Device Connector, il proxy Apache HTTP e il Rogue Detection Sensor utilizzando il metodo di installazione del pacchetto.
3. Inserire una Chiave di licenza valida o scegliere **Attiva in seguito**.
4. In caso di utilizzo di un database SQL Express, la connessione al database verrà verificata e all'utente verrà richiesto di inserire una password per ERA Web Console (passaggio 8) e la password del certificato (passaggio 10).
5. In caso di utilizzo di un sistema di database differente: Selezionare un **Account utente di servizio**. Questo account verrà utilizzato per eseguire il servizio del server ESET Remote Administrator. Le opzioni disponibili sono:

   a. Account servizio di rete
   b. Utente specificato: DOMINIO/NOME UTENTE

6. Effettuare la connessione a un database. Tutti i dati vengono memorizzati qui, dalla password della console Web ai rapporti dei computer client.

   a. Database: MySQL/MS SQL
   b. Driver ODBC: Driver MySQL ODBC 5.1/Driver Unicode MySQL ODBC 5.2/SQL Server
   c. Nome host: nome host o indirizzo IP del server del database
   d. Porta utilizzata per la connessione con il server
   e. Nome utente/password amministratore DB

Questo passaggio consentirà di verificare la connessione al database. Se la connessione è corretta, è possibile procedere al passaggio successivo.

7. Selezionare un utente per ESET Remote Administrator che ha accesso al database. È possibile utilizzare un utente esistente o crearne uno nuovo.
8. Inserire una password per l'accesso alla **Console Web**.
9. ESET Remote Administrator utilizza certificati per la comunicazione client-server. È possibile selezionare i propri certificati oppure i certificati creati dal **Server**.
10. Definire una password per l'**Autorità di certificazione. facendo attenzione a non dimenticarla.** Per creare un'autorità di certificazione per ESET Remote Administrator, fare clic su **Avanti**. Facoltativamente è possibile specificare informazioni aggiuntive sul certificato. È possibile lasciare vuoto il campo **Password dell'autorità** ma se si immette la password, **prestare attenzione a ricordarla**.

11. Fare clic su **Installa** per installare il server ERA.

12. Al termine dell'installazione, fare clic sul collegamento visualizzato nella procedura guidata di configurazione per aprire la Console Web (si consiglia di aggiungere questo URL ai segnalibri), quindi su **Fine**.

NOTA: se l'installazione termina con l'errore 2068052081, consultare il capitolo Domande frequenti per trovare una soluzione.

Installazione del proxy Remote Administrator

1. Avviare il pacchetto di installazione. Selezionare il **Proxy Remote Administrator**.
2. Selezionare i componenti che si desidera installare. Se non si dispone di un server del database, è possibile installare Microsoft SQL Server 2008 R2 Express, incluso nel pacchetto di installazione. Tenere presente che Microsoft SQL Server 2008 R2 Express prevede un limite di 10 GB per il database. È inoltre possibile installare l'RD Sensor dal pacchetto di installazione.
3. Effettuare la connessione a un database:
   a. Database: MySQL/MS SQL
   b. Driver ODBC: Driver MySQL ODBC 5.1/Driver Unicode MySQL ODBC 5.2/SQL Server
   c. Nome host: nome host o indirizzo IP del server del database
   d. Porta utilizzata per la connessione con il server
   e. Nome utente/password amministratore DB

Questo passaggio consentirà di verificare la connessione al database. Se la connessione è corretta, è possibile procedere al passaggio successivo.

4. Selezionare una porta di comunicazione del proxy. Per impostazione predefinita, verrà utilizzata la porta 2222.
5. Configurare la connessione del proxy a ESET Remote Administrator. Inserire un **Host del server** (nome host/ indirizzo IP del server) e la **Porta del server** (2222).
6. Selezionare un Certificato del peer e una password per il certificato. Aggiungere facoltativamente un'Autorità di certificazione. Questo valore deve essere inserito necessariamente solo per i certificati privi di firma.
7. Selezionare facoltativamente una cartella in cui verrà installato il Proxy e fare clic su Installa.
8. L'Agente ERA verrà installato insieme al proxy.

3.1.1 Installazione su Windows SBS/Essentials

Assicurarsi che vengano soddisfatti tutti i Requisiti, specialmente quelli relativi al Sistema operativo supportato.

NOTA: alcune versioni precedenti di Microsoft SBS, incluse le versioni di Microsoft SQL Server Express, non sono supportate da ESET Remote Administrator:

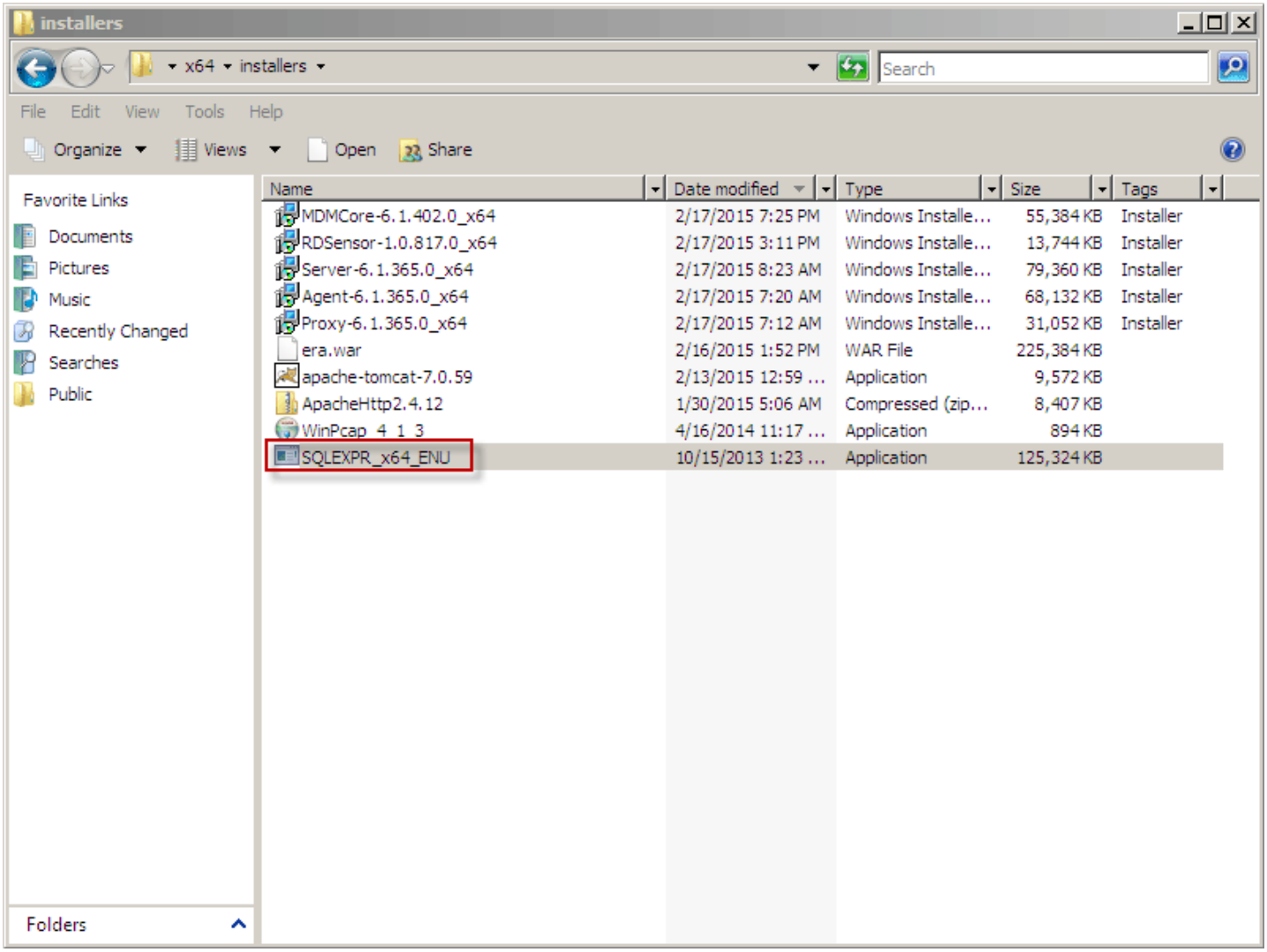
Microsoft SBS 2003 x86 SP2
Microsoft SBS 2003 x86 R2
Microsoft SBS 2008 x64 SP2

Se si è in possesso di una qualsiasi delle versioni di cui sopra di Windows Small Business Server e si desidera installare il database ERA su Microsoft SBS, è necessario utilizzare una versione più recente di Microsoft SQL Server Express.

- Se Microsoft SQL Express non è installato su SBS, seguire la procedura sottostante.
- Se Microsoft SQL Express non è installato su SBS ma non viene utilizzato, disinstallarlo e seguire la procedura sottostante.
- Se si utilizza la versione di Microsoft SQL Server Express fornita unitamente a SBS, eseguire la migrazione del database a una versione di SQL Express compatibile con il server ERA. Per eseguire questa operazione, effettuare il backup dei database, disinstallare l'installazione precedente di Microsoft SQL Server Express e seguire la procedura sottostante per installare una versione compatibile di Microsoft SQL Server Express e ripristinare i database se necessario.

1. Scaricare il pacchetto del programma di installazione ERA in un formato compresso dalla sezione dei download dei sito Web di ESET sotto a **Gestione remota** (fare clic su + per espandere la categoria).

2. Decomprimere il file del programma di installazione scaricato al passaggio uno, aprire la cartella dei programmi di installazione e fare doppio clic su **SQLEXPR_x64_ENU**.

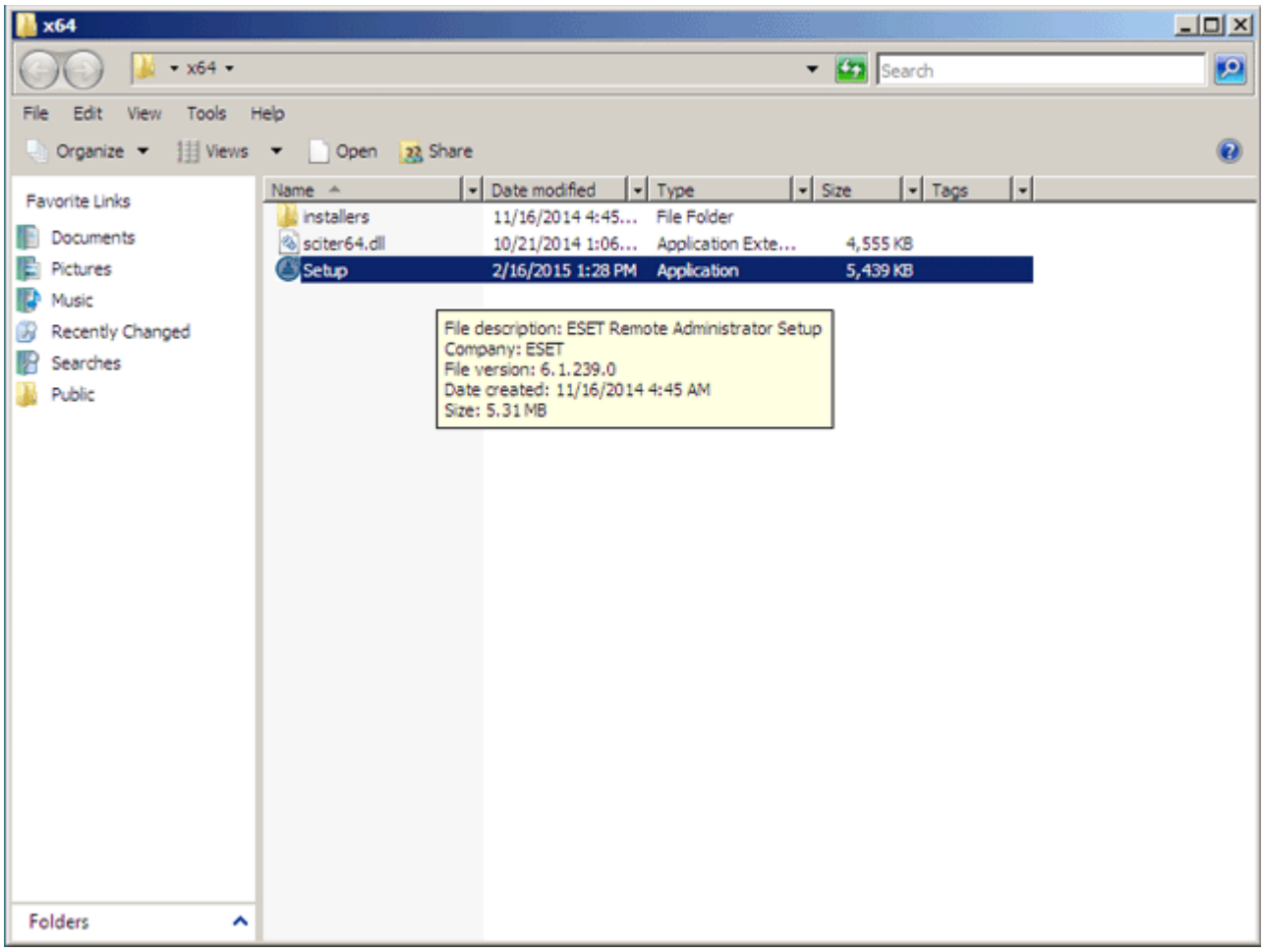

installers
x64 ▸ installers ▸
Search
File Edit View Tools Help
Organize Views Open Share
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders
Name
Date modified
Type
Size
Tags
MDMCore-6.1.402.0_x64 2/17/2015 7:25 PM Windows Installe... 55,384 KB Installer
RDSensor-1.0.817.0_x64 2/17/2015 3:11 PM Windows Installe... 13,744 KB Installer
Server-6.1.365.0_x64 2/17/2015 8:23 AM Windows Installe... 79,360 KB Installer
Agent-6.1.365.0_x64 2/17/2015 7:20 AM Windows Installe... 68,132 KB Installer
Proxy-6.1.365.0_x64 2/17/2015 7:12 AM Windows Installe... 31,052 KB Installer
era.war 2/16/2015 1:52 PM WAR File 225,384 KB
apache-tomcat-7.0.59 2/13/2015 12:59 ... Application 9,572 KB
ApacheHttp2.4.12 1/30/2015 5:06 AM Compressed (zip... 8,407 KB
WinPcap_4_1_3 4/16/2014 11:17 ... Application 894 KB
SQLEXPR_x64_ENU 10/15/2013 1:23 ... Application 125,324 KB

- All'apertura del Centro di installazione, fare clic su **Nuova installazione o aggiungere funzioni a un'installazione esistente** per avviare la procedura guidata di installazione.

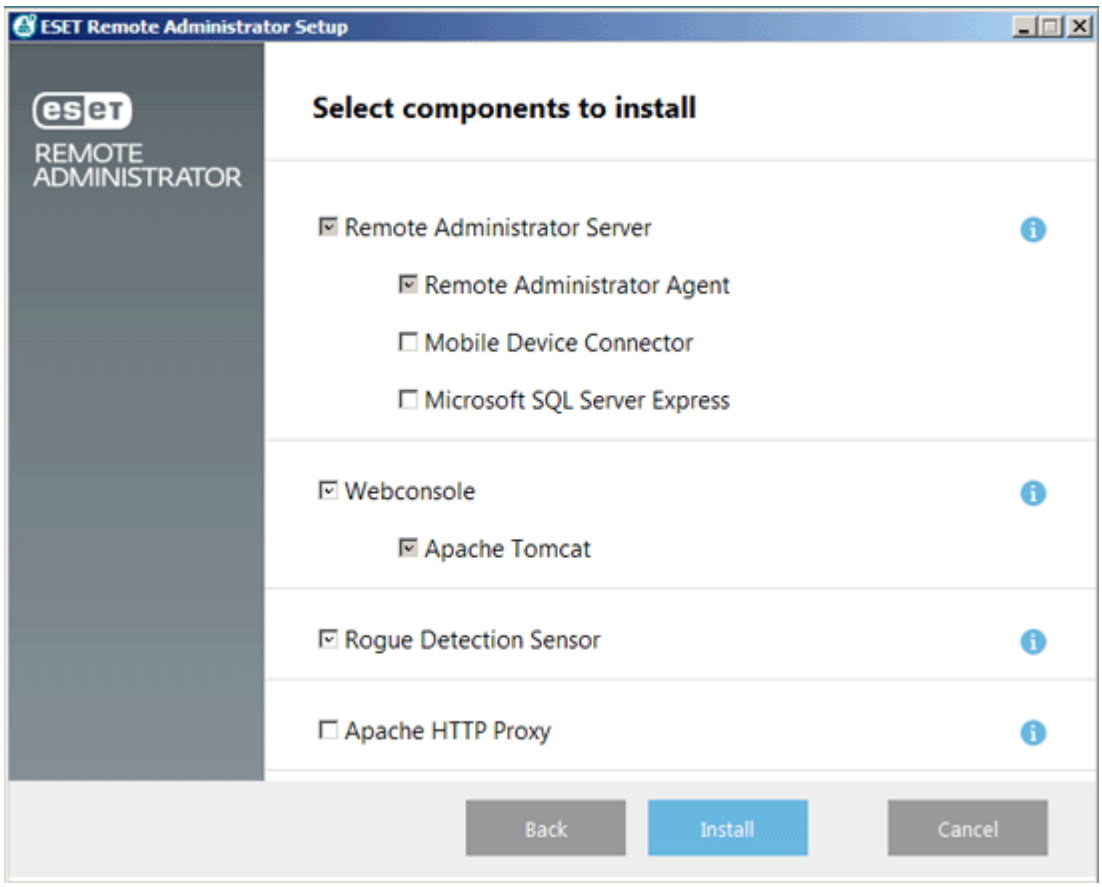
NOTA: nel passaggio 8 del processo di installazione, impostare la modalità di autenticazione su **Modalità mista (autenticazione di SQL Server e autenticazione di Windows)**.

NOTA: per installare il server ERA su SBS, è necessario consentire le connessioni TCP/IP su SQL Server.

3. Installare ESET Remote Administrator mediante l'esecuzione di **Setup.exe**.



4. Selezionare i componenti che si desidera installare, assicurarsi di deselezionare Microsoft SQL Server Express e fare clic su **Installa**.



3.2 Database

ESET Remote Administrator utilizza un database per archiviare i dati del client. Nelle sezioni che seguono vengono illustrati in dettaglio il processo di installazione, backup, aggiornamento e migrazione del database del server/proxy ERA:

- Rivedere la compatibilità del database e i requisiti di sistema per il server ERA.
- Se non è stato configurato un database da utilizzare con il server ERA, tenere presente che **Microsoft SQL Server Express** è incluso nel programma di installazione.
- Se si utilizza Microsoft Small Business Server (SBS) o Essentials, si consiglia di assicurarsi che vengano soddisfatti tutti i requisiti e che si stia utilizzando un sistema operativo supportato. Se vengono soddisfatti tutti i requisiti, seguire le istruzioni per l'installazione per Windows SBS/Essentials per installare ERA su questi sistemi operativi.
- Se sul sistema in uso è installato Microsoft SQL Server, rivedere i requisiti per assicurarsi che la versione di Microsoft SQL Server sia supportata da ESET Remote Administrator. Se la versione di Microsoft SQL Server non è supportata, effettuare l'aggiornamento a una versione compatibile di SQL Server.

3.2.1 Backup del server del database

Tutte le informazioni e le impostazioni relative a ESET Remote Administrator vengono salvate in un database. Si consiglia di effettuare backup periodici del database al fine di prevenire la perdita di dati. Consultare la sezione appropriata al database in uso tra quelle sottostanti:

- MySQL
- SQL Server

Il backup può anche essere utilizzato in un momento successivo durante la migrazione di ESET Remote Administrator in un nuovo server.

Se si desidera ripristinare il backup del database, seguire la procedura sottostante:

- MySQL
- SQL Server

3.2.2 Aggiornamento del server del database

Seguire le istruzioni sottostanti per aggiornare un'istanza esistente di Microsoft SQL Server a una nuova versione da utilizzare con il database del server ERA o del proxy ERA:

1. **Interrompere** tutti i servizi del server ERA o del proxy ERA in esecuzione che si connettono al server del database da aggiornare. Interrompere anche qualsiasi altra applicazione che potrebbe connettersi all'istanza di Microsoft SQL Server.
2. Eseguire il backup di tutti i database contenuti prima di procedere.
3. Eseguire l'aggiornamento del server del database in base alle istruzioni del fornitore.
4. **Avviare** tutti i servizi del server ERA e/o del proxy ERA e controllarne i registri di traccia per verificare che la connessione del database funzioni correttamente.

Per ulteriori informazioni relative al database, consultare le seguenti pagine Web:

- Eseguire l'aggiornamento a SQL Server https://msdn.microsoft.com/it-it/library/bb677622.aspx (è possibile fare clic su **Altre versioni** per consultare le istruzioni per l'aggiornamento di una specifica versione di SQL Server)
- Aggiornare MySQL Server (alla versione 5.6) http://dev.mysql.com/doc/refman/5.6/en/upgrading.html

3.2.3 Migrazione del database ERA

Fare clic sul collegamento sottostante appropriato per consultare le istruzioni sulle modalità di migrazione del database del server ERA o del proxy ERA tra diverse istanze di SQL Server (ciò vale anche in caso di migrazione verso un'altra versione di SQL Server o un SQL Server ospitato su un'altra macchina):

- Processo di migrazione per SQL Server
- Processo di migrazione per MySQL Server

3.2.3.1 Processo di migrazione per SQL Server

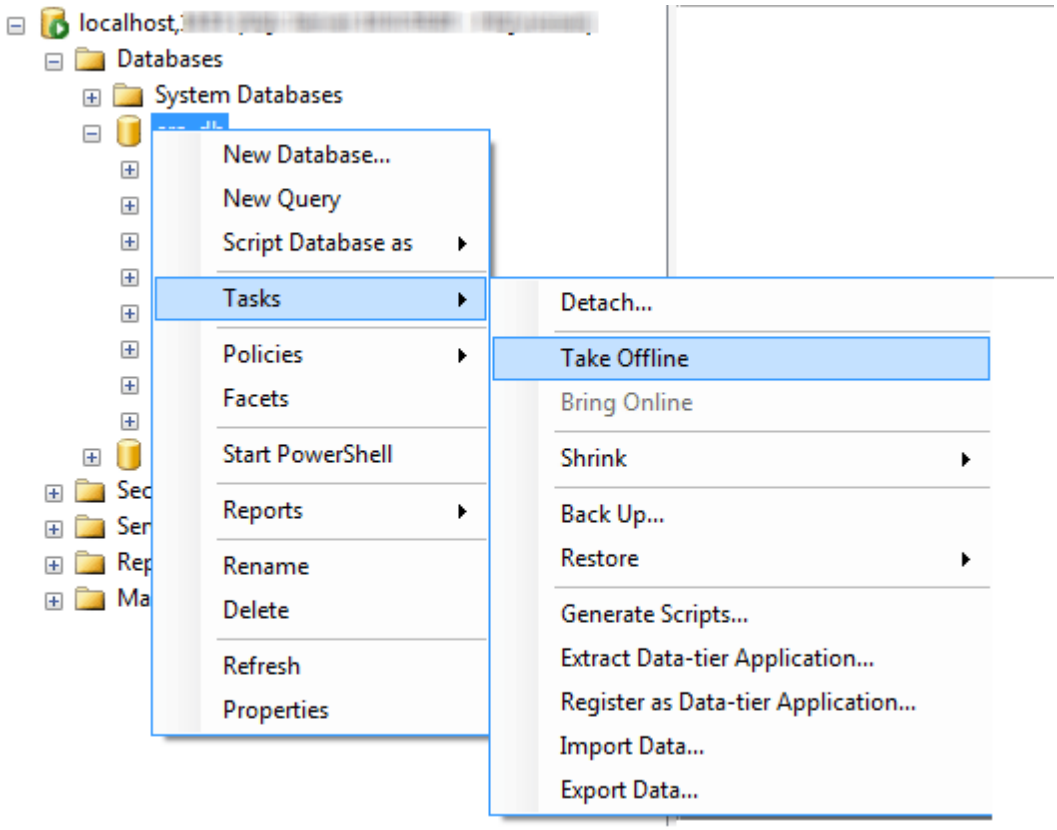
Questo processo di migrazione è identico a quello relativo a **Microsoft SQL Server** e **Microsoft SQL Server Express**.

Per ulteriori informazioni, consultare il seguente articolo della Knowledge Base di Microsoft: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

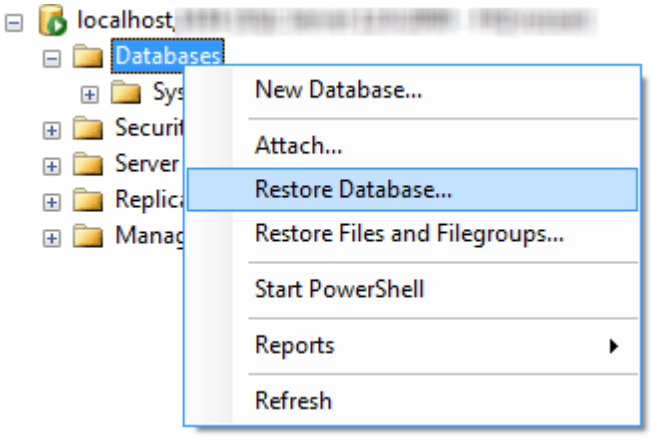
- **Prerequisiti:**
  - È necessario installare le istanze di origine e di destinazione di SQL Server, che possono essere ospitate su macchine diverse.
  - L'istanza di destinazione di SQL Server deve avere almeno la stessa versione di quella di origine. **Il ripristino della versione precedente non è supportato.**
  - È necessario installare **SQL Server Management Studio**. Se le istanze di SQL Server si trovano su macchine diverse, è necessario che il software sia presente su entrambe.

- **Migrazione:**

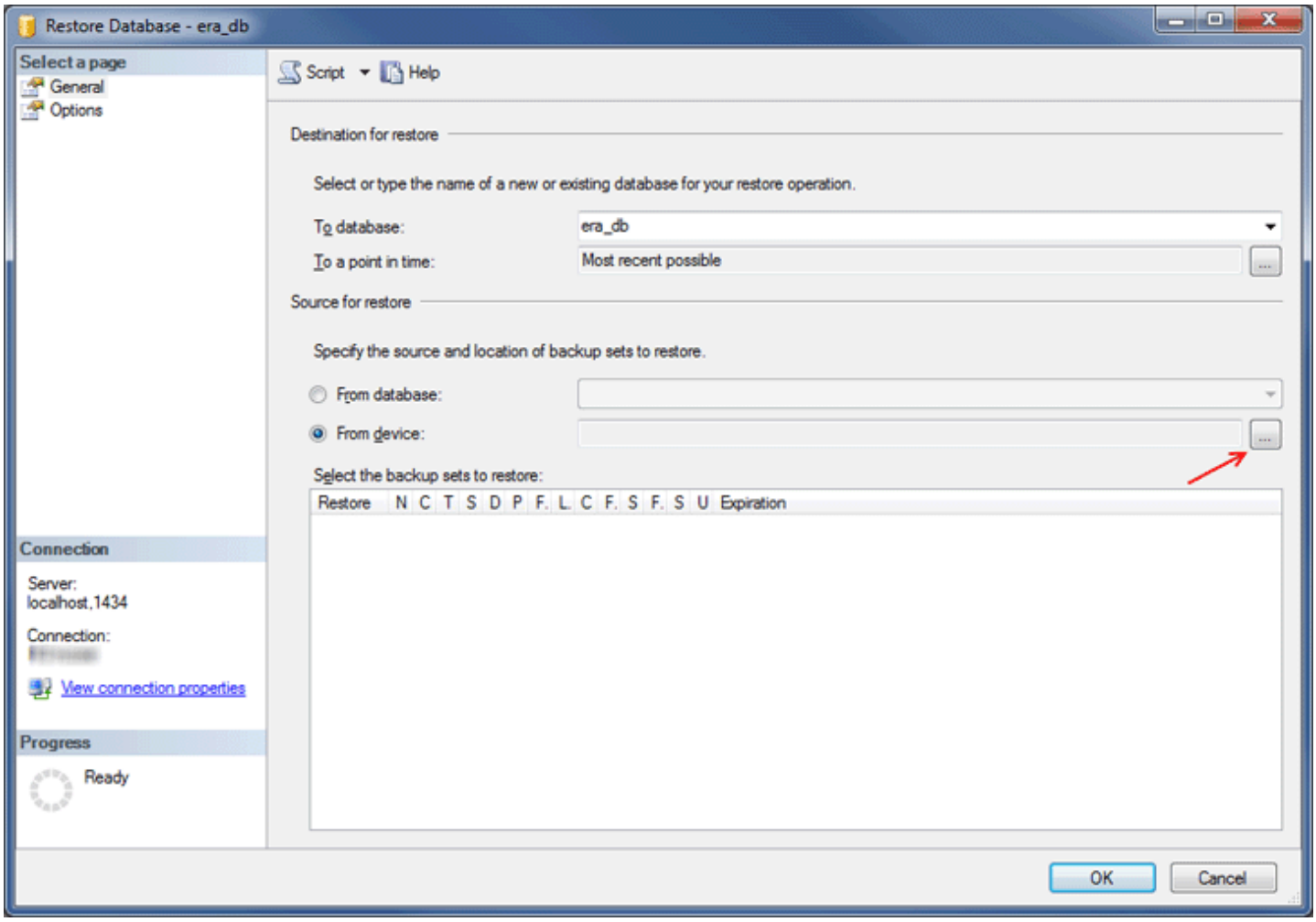
1. **Interrompere** il servizio del server ERA o del proxy ERA.
2. Accedere all'istanza di origine di SQL Server mediante SQL Server Management Studio.
3. **Creare** un backup completo del database per il quale effettuare la migrazione. Si consiglia di specificare un nuovo nome per il set di backup. In alternativa, se il set di backup è già stato utilizzato, verrà aggiunto il nuovo backup e ciò determinerà la creazione di un file di backup inutilmente grande.
4. Mettere il database di origine off-line selezionando **Attività** > **Metti off-line**.



5. **Copiare** il file di backup (.bak) creato nel passaggio 3 in un punto accessibile dall'istanza di destinazione di SQL Server. Per il file di backup del database potrebbe essere necessario modificare i diritti di accesso.
6. **Portare** il database di origine nuovamente on-line ma **non avviare ancora il server ERA!**
7. Accedere all'istanza di destinazione di SQL Server con SQL Server Management Studio.
8. Ripristinare il database sull'istanza di destinazione di SQL Server.



9. Digitare un nome per il nuovo database nel campo del database "A". In base alle preferenze dell'utente, è possibile utilizzare lo stesso nome del vecchio database.
10. Selezionare **Dal dispositivo** sotto a **Specifica i set di backup di origine e la relativa posizione per effettuare il ripristino** , quindi fare clic su **...** .

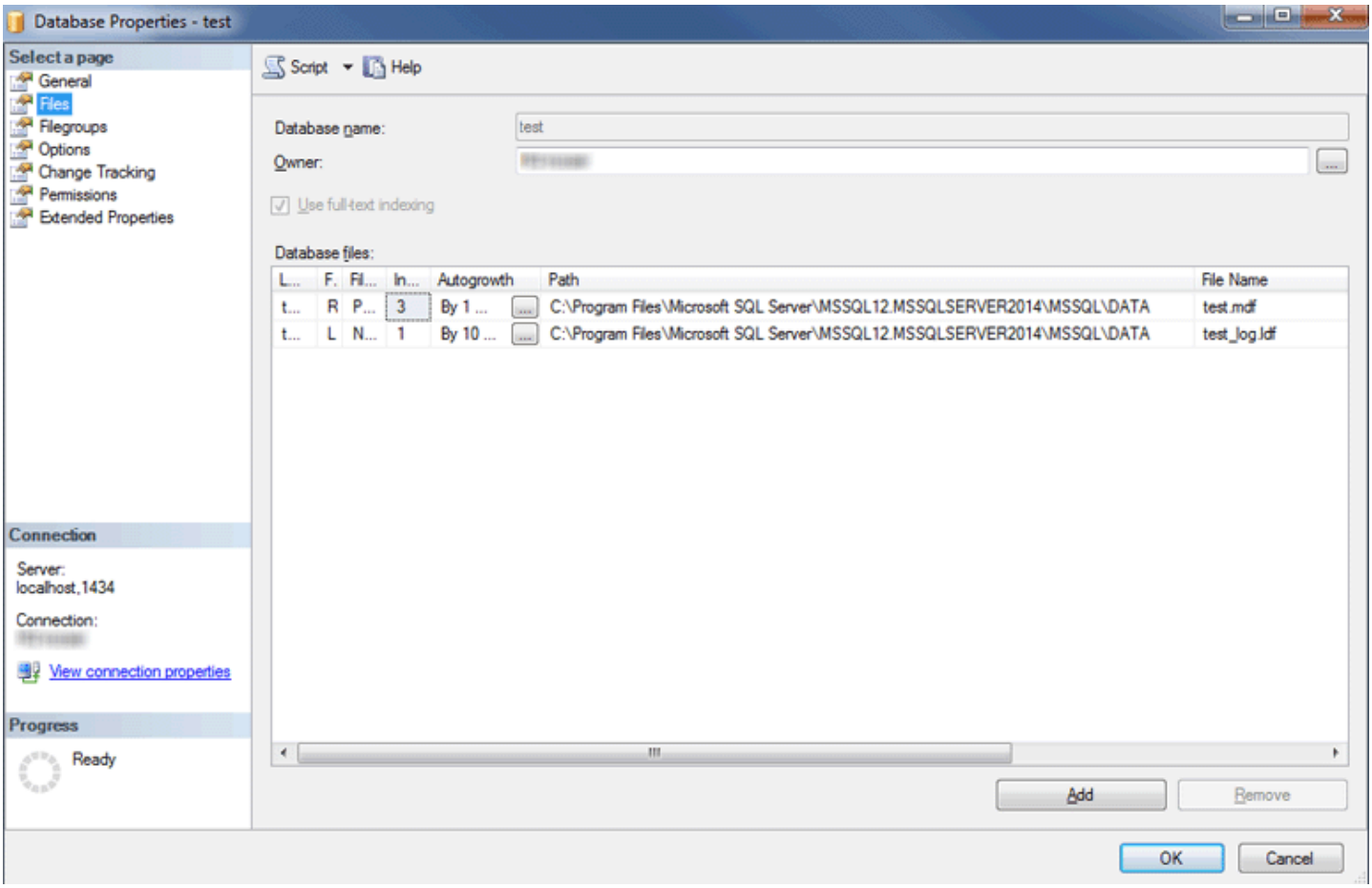


11. Fare clic su **Aggiungi**, accedere al file di backup e aprirlo.

12. Selezionare il backup più recente possibile per effettuare il ripristino (il set di backup può contenere backup multipli).

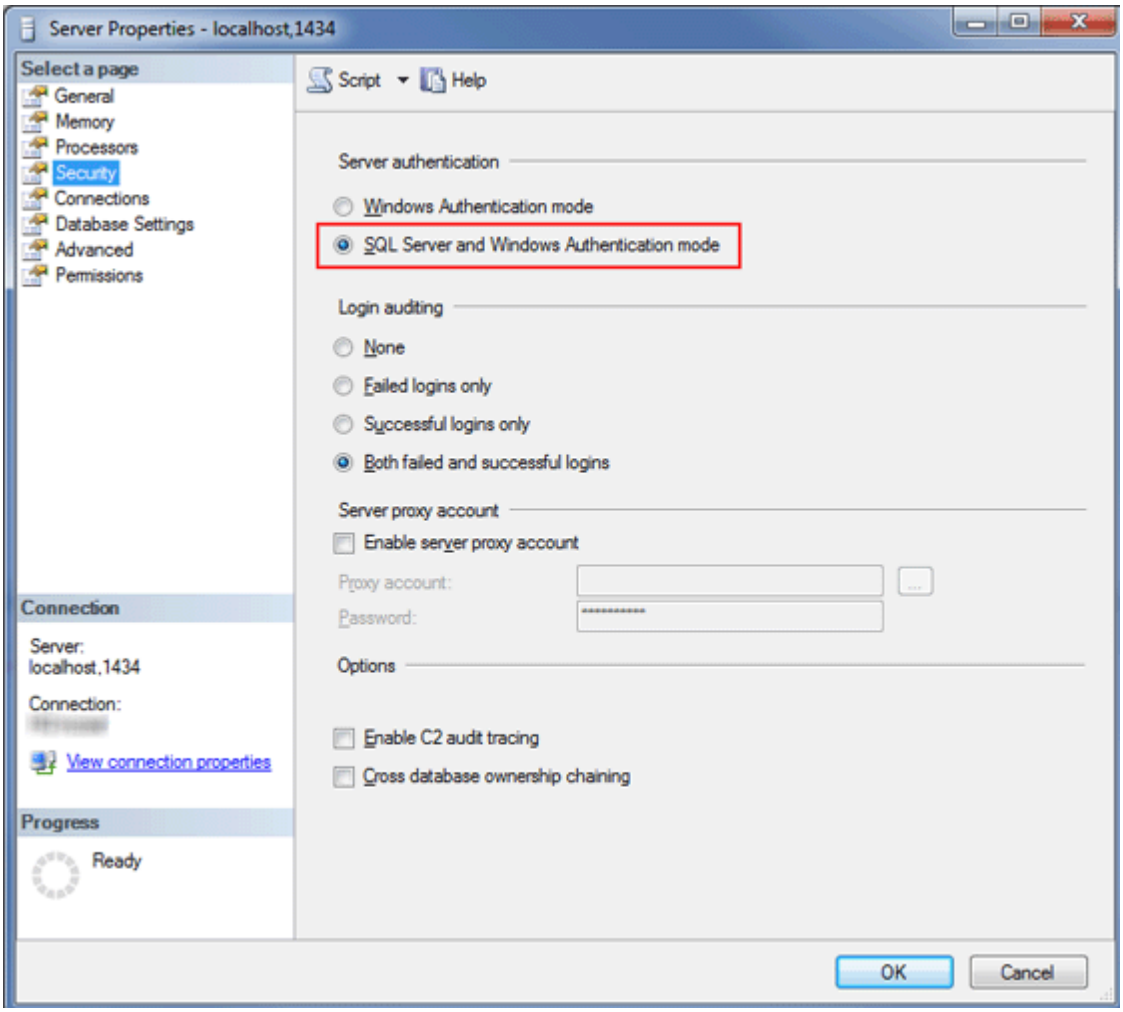
13. Fare clic sulla pagina delle **Opzioni** della procedura guidata di ripristino. Facoltativamente, selezionare **Sovrascrivi il database esistente** e assicurarsi che i punti di ripristino per il database (`.mdf`) e per il rapporto (`.ldf`) siano corretti. Lasciando i valori predefiniti inalterati, verranno utilizzati i percorsi dall'istanza di origine di SQL Server. Si prega pertanto di controllare questi valori.

    - Se non si è sicuri del punto di archiviazione dei file del DB sull'istanza di destinazione di SQL Server, fare clic con il pulsante destro del mouse su un database esistente, selezionare **Proprietà** e fare clic sulla scheda **File**. La directory in cui è archiviato il database è visualizzata nella colonna **Percorso** della tabella visualizzata di seguito.

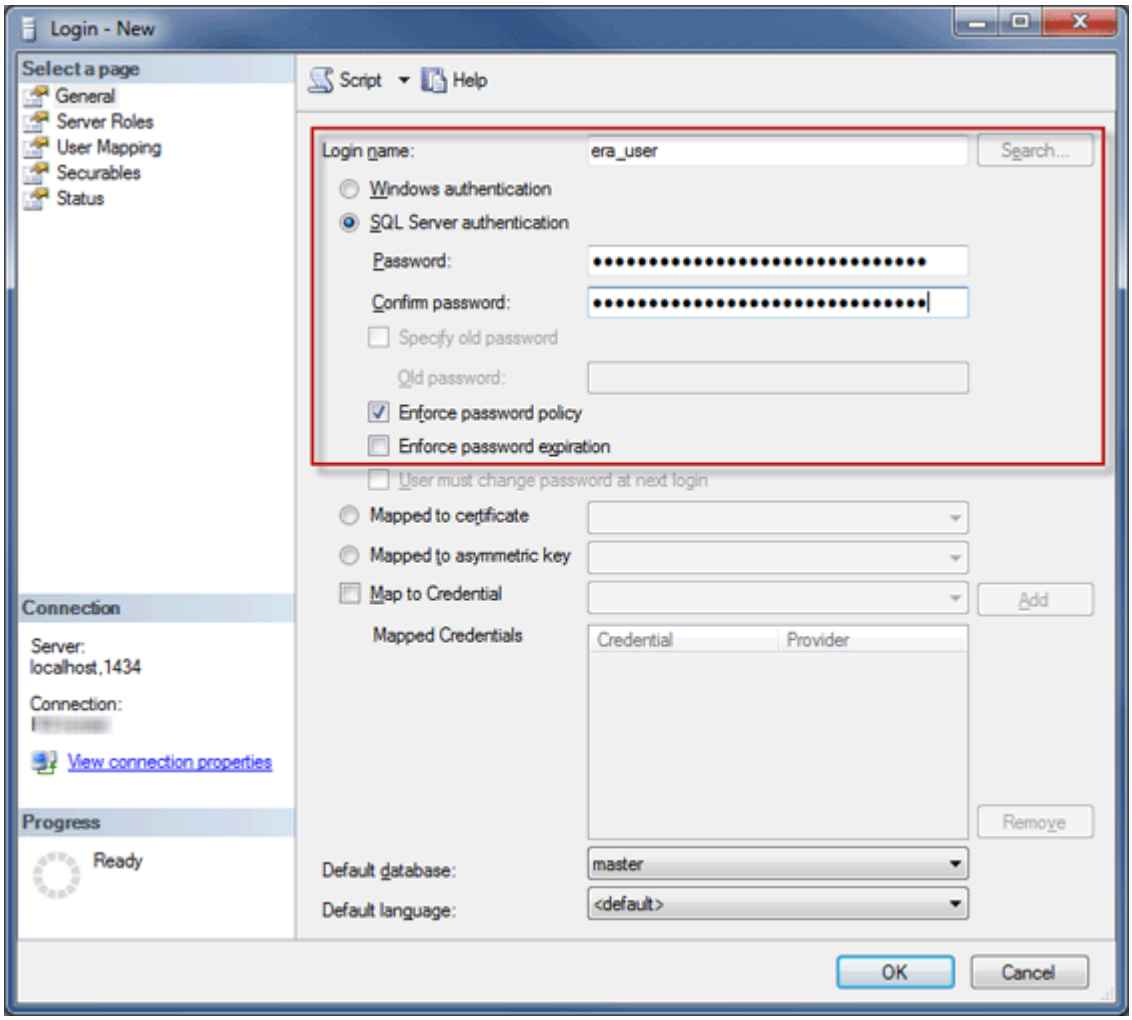


14. Fare clic su **OK** nella finestra della procedura guidata di ripristino.

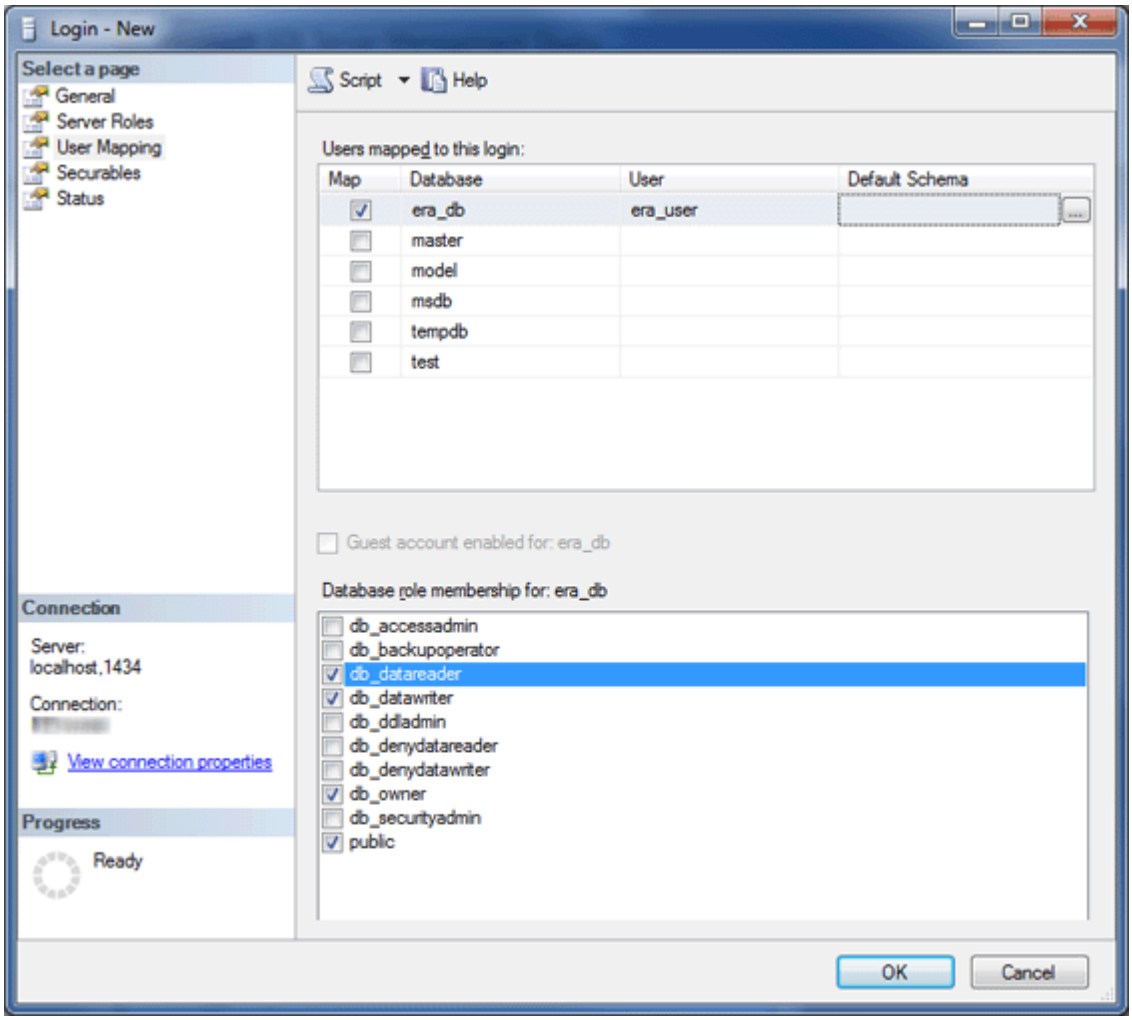
15. Assicurarsi che sul nuovo server del database **sia attiva l'autenticazione di SQL Server**. Fare clic con il pulsante destro del mouse sul server, quindi su **Proprietà**. Accedere a **Sicurezza** e verificare che sia selezionata la modalità di autenticazione di SQL Server e Windows.



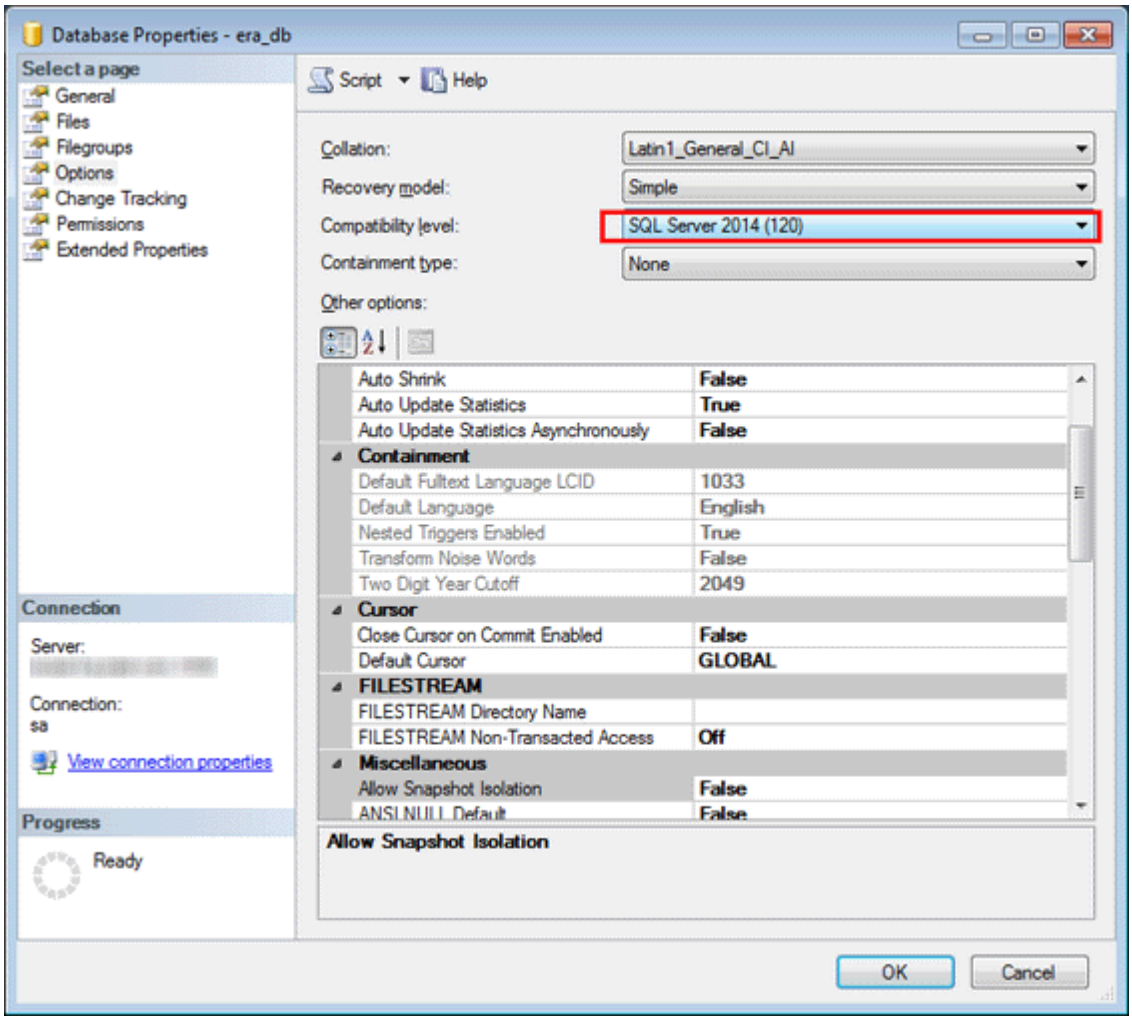
16. **Creare un nuovo accesso per SQL Server** (per il server/proxy ERA) nell'istanza di destinazione di SQL Server con l'**Autenticazione di SQL Server** ed eseguire il mapping dell'accesso a un utente nel database ripristinato.
    - Non attivare la scadenza della password.
    - Caratteri consigliati per i nomi utente:
        - lettere ASCII minuscole, numeri e carattere di sottolineatura "_"
    - Caratteri raccomandati per le password:
        - SOLO caratteri ASCII, incluse lettere ASCII minuscole e maiuscole, numeri, spazi, caratteri speciali
    - Non utilizzare caratteri non-ASCII come parentesi graffe {} e @
    - Si tenga presente che, in caso di mancata osservanza delle raccomandazioni sui caratteri di cui sopra, potrebbero verificarsi problemi di connettività del database oppure sarà necessario effettuare l'escape dei caratteri speciali nei passaggi successivi durante la modifica delle stringhe di connessione del database. In questo documento non vengono illustrate le regole per effettuare l'escape dei caratteri.



17. Effettuare il mapping dell'accesso a un utente del database di destinazione. Nella scheda dei mapping dell'utente, assicurarsi che l'utente del database sia in possesso dei seguenti ruoli: **db_datareader**, **db_datawriter**, **db_owner**.



18. Per attivare le ultime funzioni del server del database, modificare il **Livello di compatibilità** del database ripristinato aggiornandolo all'ultima versione. Fare clic con il pulsante destro del mouse sul nuovo database e aprire le **Proprietà** del database.



NOTA: SQL Server Management Studio non è in grado di definire livelli di compatibilità successivi a quelli della versione in uso. Ad esempio, SQL Server Management Studio 2008 non è in grado di impostare il livello di compatibilità per SQL Server 2014.

19. **Trovare** `startupconfiguration.ini` sulla macchina su cui è installato il server/proxy ERA.

- Per Windows Vista e versioni successive:
  % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
- Per le versioni di Windows precedenti:
  % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
- Per Linux:
  /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

20. **Modificare** la stringa di connessione del database nel server/proxy ERA startupconfiguration.ini

- Impostare l'indirizzo e la porta del nuovo server del database.
- Impostare il nuovo nome utente e la password ERA nella stringa di connessione.
  - Il risultato finale dovrebbe essere il seguente:

```
DatabaseType=MSSQLOdbc
DatabaseConnectionString=Driver=SQL Server;Server=localhost,1433;Uid=era_user1;Pwd={SecretPassword123
```

21. **Avviare** il server/proxy ERA e verificare che il relativo servizio venga eseguito correttamente.

3.2.3.2 Processo di migrazione per MySQL Server

- **Prerequisiti:**
  - È necessario installare le istanze di origine e di destinazione di SQL Server, che possono essere ospitate su macchine diverse.
  - Gli strumenti MySQL devono essere disponibili almeno su uno dei computer (client mysqldump e mysql).

- **Collegamenti utili:**

http://dev.mysql.com/doc/refman/5.6/en/copying-databases.html

http://dev.mysql.com/doc/refman/5.6/en/mysqldump.html

http://dev.mysql.com/doc/refman/5.6/en/mysql.html

- Nei comandi, nei file di configurazione o nelle dichiarazioni di SQL sottostanti, sostituire sempre:
  - **SRCHOST** con l'indirizzo dell'istanza di origine del server del database
  - **SRCROOTLOGIN** con l'accesso dell'utente radice dell'istanza di origine di MySQL Server
  - **SRCERADBNAME** con il nome dell'istanza di origine del database ERA per il quale eseguire il backup
  - **BACKUPFILE** con il percorso al file in cui verrà archiviato il backup
  - **TARGETHOST** con l'indirizzo dell'istanza di destinazione del server del database
  - **TARGETROOTLOGIN** con l'accesso dell'utente radice dell'istanza di destinazione di MySQL Server
  - **TARGETERADBNAME** con il nome dell'istanza di destinazione del database ERA (in seguito alla migrazione)
  - **TARGETERALOGIN** con il nome di accesso per il nuovo utente del database ERA sull'istanza di destinazione di MySQL Server
  - **TARGETERAPASSWD** con la password del nuovo utente del database ERA sull'istanza di destinazione di MySQL Server

Non è necessario eseguire le dichiarazioni SQL sottostanti attraverso la riga di comando. Se è disponibile lo strumento GUI, è possibile utilizzare un'applicazione già nota.

1. **Interrompere** i servizi del server/proxy ERA.
2. **Creare** un backup completo dell'istanza di origine del database ERA (database che si desidera migrare):
   ```
   mysqldump --host SRCHOST --disable-keys --extended-insert -u SRCROOTLOGIN -p SRCERADBNAME > BACKUPFILE
   ```
3. **Preparare** un database vuoto sull'istanza di destinazione di MySQL Server:
   ```
   mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE DATABASE TARGETERADBNAME /*!40100 DEFAUL
   ```

NOTA: utilizzare il carattere apostrofo ' al posto delle virgolette " sui sistemi Linux.

4. **Ripristinare** il database sull'istanza di destinazione di MySQL Server sul database vuoto preparato in precedenza:
   ```
   mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETERADBNAME < BACKUPFILE
   ```
5. **Creare** un utente per il database ERA sull'istanza di destinazione di MySQL Server:
   ```
   mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE USER TARGETERALOGIN@'%' IDENTIFIED BY 'TA
   ```

Caratteri raccomandati per **TARGETERALOGIN**:
- lettere ASCII minuscole, numeri e sottolineatura "_"

Caratteri raccomandati per **TARGETERAPASSWD**:
- solo caratteri ASCII, incluse lettere ASCII minuscole e maiuscole, numeri, spazi e caratteri speciali
- Non utilizzare caratteri non-ASCII, parentesi graffe {} o @

Si tenga presente che, in caso di mancata osservanza delle raccomandazioni sui caratteri di cui sopra, potrebbero verificarsi problemi di connettività del database oppure sarà necessario effettuare l'escape dei caratteri speciali nei passaggi successivi durante la modifica delle stringhe di connessione del database. In questo documento non vengono illustrate le regole per effettuare l'escape dei caratteri.

6. **Garantire** adeguati diritti di accesso all'utente del database ERA sull'istanza di destinazione di MySQL Server:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=GRANT ALL ON TARGETERADBNAME.* TO TARGETERALOGIN
```

NOTA: utilizzare il carattere apostrofo ' al posto delle virgolette " sui sistemi Linux.

7. **Trovare** `startupconfiguration.ini` sulla macchina su cui è installato il server/proxy ERA.
   - Per Windows Vista e versioni successive:
     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - Per le versioni di Windows precedenti:
     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - Per Linux:
     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
8. **Modificare** la stringa di connessione del database nel server/proxy ERA `startupconfiguration.ini`
   - Impostare l'indirizzo e la porta del nuovo server del database
   - Impostare il nome utente e la password
     - Il risultato finale dovrebbe essere il seguente:
```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETERAI
```
9. **Avviare** il server/proxy ERA e verificare che il relativo servizio venga eseguito correttamente.

3.3 Immagine ISO

Un file di immagine ISO è uno dei formati in cui è possibile scaricare i programmi di installazione (categoria dei programmi di installazione integrati) di ESET Remote Administrator. L'immagine ISO contiene i seguenti elementi:

- Pacchetto di installazione ERA
- Programmi di installazione separati per ciascun componente

L'immagine ISO è utile nel momento in cui si desidera mantenere tutti i programmi di installazione di ESET Remote Administrator in un'unica posizione. Questo strumento consente inoltre di eliminare il bisogno di scaricare i programmi di installazione dal sito Web di ESET tutte le volte che si desidera eseguire l'installazione. L'immagine ISO è inoltre utile se si desidera installare ESET Remote Administrator su una macchina virtuale.

3.4 Accessori virtuali

Il server ERA si presta a essere utilizzato in un ambiente VMware o Microsoft Hyper-V. ERA Virtual Appliance si presenta sotto forma di file OVA (Open Virtualization Appliance). Il file OVA è un modello che contiene un sistema operativo CentOS 6.5 funzionale. È possibile utilizzare il server ERA, proxy ERA o ERA MDM attraverso il modello appropriato. Prima dell'utilizzo di un modello OVF in VMware, seguire le istruzioni fornite nella procedura guidata per specificare la password per l'account di amministratore ERA e configurare la macchina virtuale. Dopo aver utilizzato gli accessori, la macchina virtuale si trasforma in un ambiente completo in cui ESET Remote Administrator è pronto all'uso.

Gli accessori virtuali di ERA sono del tipo della famiglia hardware virtuale vmx-07 e supportati dai seguenti hypervisor VMware:

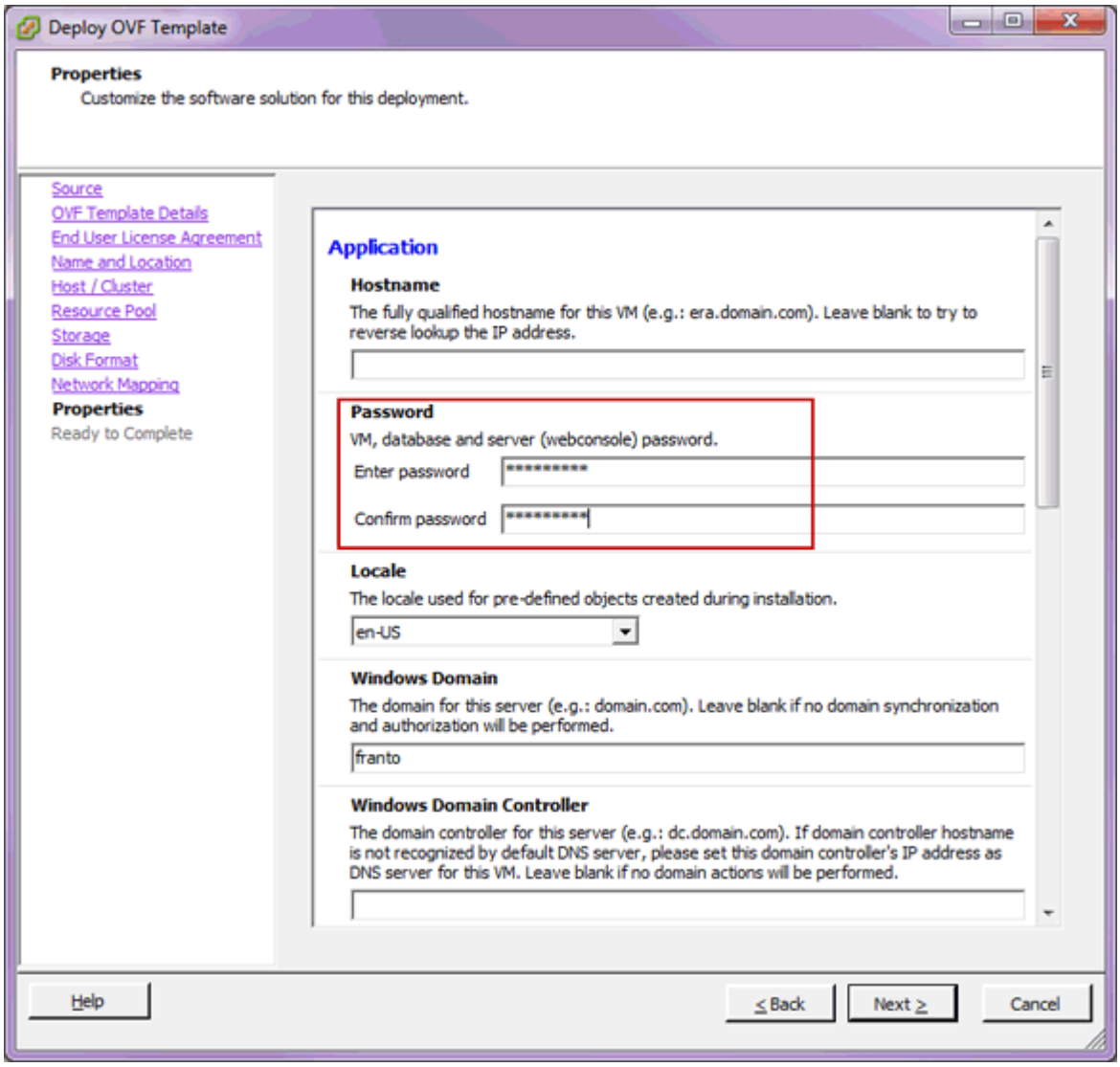
- ESXi 5.0 e versioni successive
- Workstation 6.5 e versioni successive

È possibile utilizzare VMware Player o Oracle VirtualBox su un sistema operativo desktop e distribuire gli accessori virtuali tramite tale configurazione. In questo modo è possibile eseguire ESET Remote Administrator su un sistema operativo non server senza la necessità di utilizzare ESXi a livello aziendale. Ciò vale solo per il file `ERA_Server.ova`.

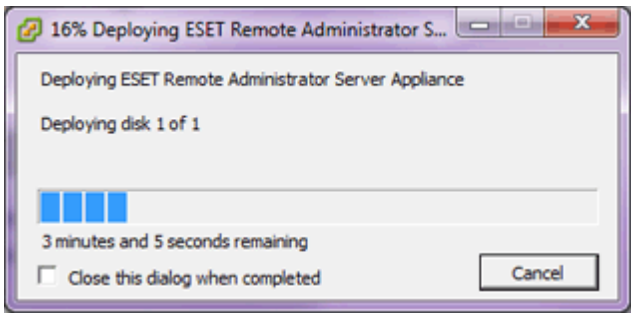
Utilizzo di un modello OVF nel client vSphere

1. Effettuare la connessione al server vCenter utilizzando il client vSphere (non effettuare la connessione diretta al server ESXi).
2. Fare clic su **File** sulla barra dei menu in alto e selezionare **Utilizza modello OVF**.
3. Fare clic su **Sfoglia**, accedere al file OVA scaricato dal sito Web di ESET e fare clic su Apri. In base al componente che si desidera impiegare, utilizzare di conseguenza il file `ERA_Server.ova` `ERA_Proxy.ova` o `ERA_MDM.ova`.
4. Fare clic su **Avanti** nella finestra Dettagli del modello OVF.
5. Leggere e accettare l'Accordo di licenza per l'utente finale (ALUF).
6. Seguire le istruzioni a schermo per completare l'installazione e specificare le informazioni seguenti sul client virtuale in uso:
   - Nome e posizione
   - Host/Cluster
   - Pool di risorse
   - Archiviazione
   - Formato disco
   - Mappatura rete
6. Nella pagina **Proprietà**, specificare il **Nome host** (che sarà il nome host del server ERA o del proxy ERA) e una **Password**. Questa password è importante poiché verrà utilizzata in tutti i componenti ERA: database ERA, server ERA ed ERA Web Console, oltre che per l'accesso alla macchina virtuale ERA (CentOS).

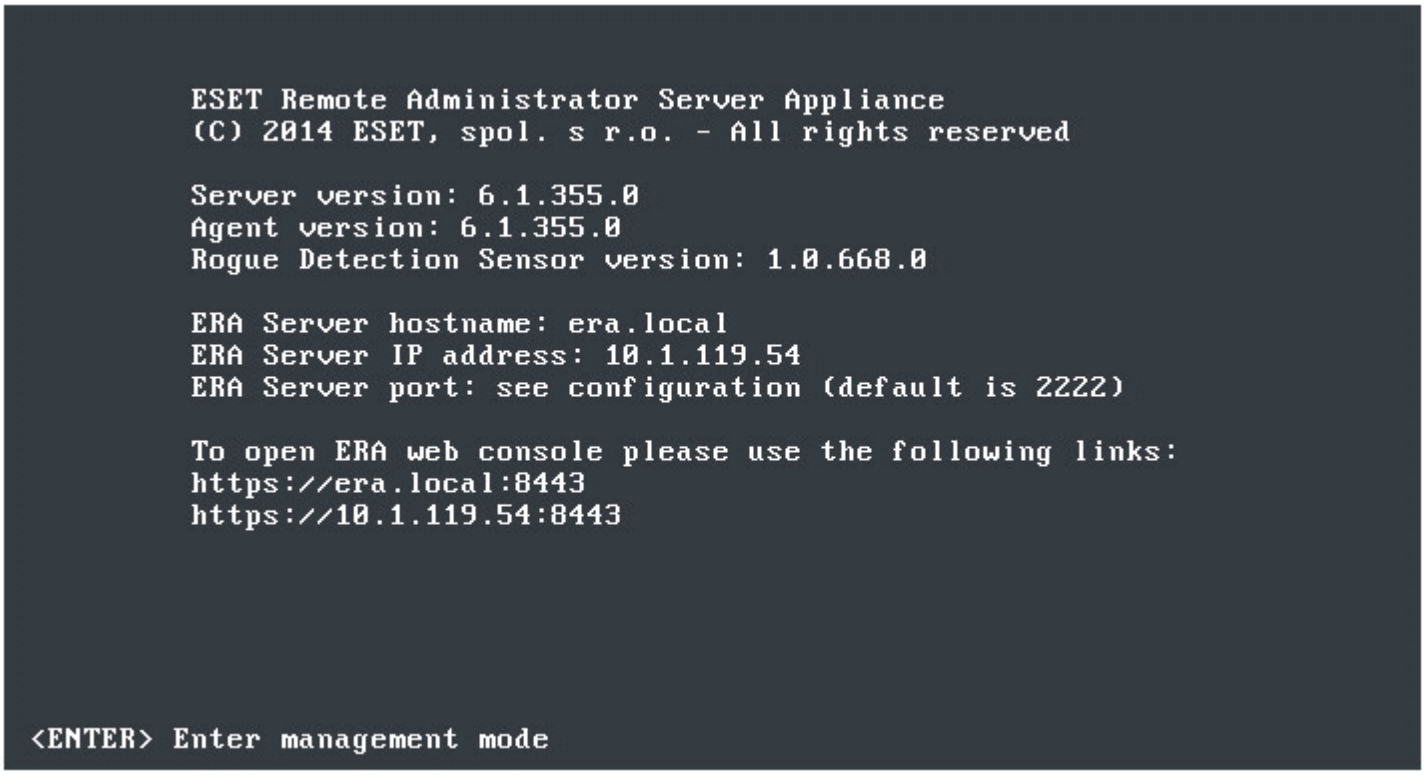
7. I restanti campi sono facoltativi: è possibile specificare i dettagli del **Dominio Windows** che risultano utili per la Sincronizzazione dei gruppi statici. È inoltre possibile impostare le **Proprietà di rete**.


Deploy OVF Template
Properties
Customize the software solution for this deployment.
Source
OVF Template Details
End User License Agreement
Name and Location
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Application
Hostname
The fully qualified hostname for this VM (e.g.: era.domain.com). Leave blank to try to reverse lookup the IP address.
Password
VM, database and server (webconsole) password.
Enter password
Confirm password
Locale
The locale used for pre-defined objects created during installation.
en-US
Windows Domain
The domain for this server (e.g.: domain.com). Leave blank if no domain synchronization and authorization will be performed.
franto
Windows Domain Controller
The domain controller for this server (e.g.: dc.domain.com). If domain controller hostname is not recognized by default DNS server, please set this domain controller's IP address as DNS server for this VM. Leave blank if no domain actions will be performed.
Help
< Back
Next >
Cancel

8. Fare clic su **Avanti**, rivedere il riepilogo relativo alla distribuzione e fare clic su **Fine**. Il processo creerà automaticamente una macchina virtuale con le impostazioni specificate. Al termine della corretta creazione della VM, è possibile accenderla.


16% Deploying ESET Remote Administrator S...
Deploying ESET Remote Administrator Server Appliance
Deploying disk 1 of 1
3 minutes and 5 seconds remaining
Close this dialog when completed
Cancel

9. All'apertura della console VMware dopo la distribuzione di ERA, verranno visualizzate le seguenti informazioni dell'URL di ERA Web Console nel formato https://[IP address]:8443. Immettere l'URL visualizzato nel browser Web per poter accedere a ERA Web Console (utilizzare la password specificata al passaggio 6).


ESET Remote Administrator Server Appliance
(C) 2014 ESET, spol. s r.o. - All rights reserved
Server version: 6.1.355.0
Agent version: 6.1.355.0
Rogue Detection Sensor version: 1.0.668.0
ERA Server hostname: era.local
ERA Server IP address: 10.1.119.54
ERA Server port: see configuration (default is 2222)
To open ERA web console please use the following links:
https://era.local:8443
https://10.1.119.54:8443
<ENTER> Enter management mode

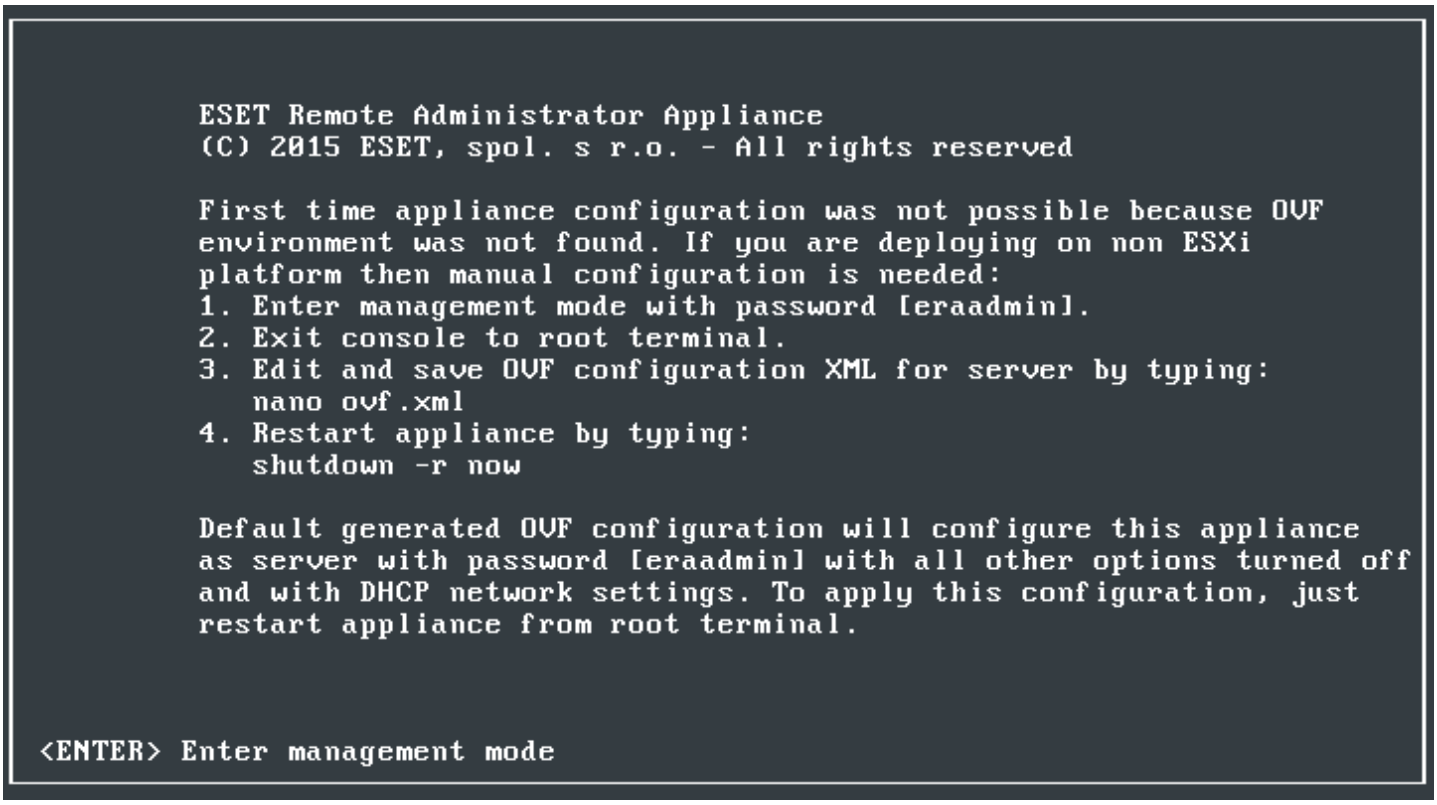
NOTA: si consiglia vivamente di configurare i ruoli e le autorizzazioni di vCenter in modo tale che gli utenti VMware non riescano ad accedere alla macchina virtuale ERA. In questo modo si impedisce agli utenti di manomettere ERA VM. Non è necessario che gli utenti ERA accedano alla VM. Per gestire l'accesso a ESET Remote Administrator, utilizzare i Diritti di accesso all'interno di ERA Web Console.

3.4.1 VMware Player

Utilizzo di un modello OVF in VMware Player

Si consiglia di utilizzare la versione più recente di VMware Player.

1. Selezionare **File** > **Apri una macchina virtuale**.
2. Accedere al file OVA (`ERA_Server.ova`) scaricato dal sito Web di ESET. Fare clic su **Apri**.
3. Fornire un nome e il percorso di archiviazione locale della nuova macchina virtuale e fare clic su **Importa.**
4. Leggere e accettare eventualmente l'Accordo di licenza per l'utente finale (ALUF).
5. Dopo aver eseguito la distribuzione degli accessori, è possibile attivarli. Verranno visualizzate le seguenti informazioni:


ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved
First time appliance configuration was not possible because OVF environment was not found. If you are deploying on non ESXi platform then manual configuration is needed:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
nano ovf.xml
4. Restart appliance by typing:
shutdown -r now
Default generated OVF configuration will configure this appliance as server with password [eraadmin] with all other options turned off and with DHCP network settings. To apply this configuration, just restart appliance from root terminal.
<ENTER> Enter management mode

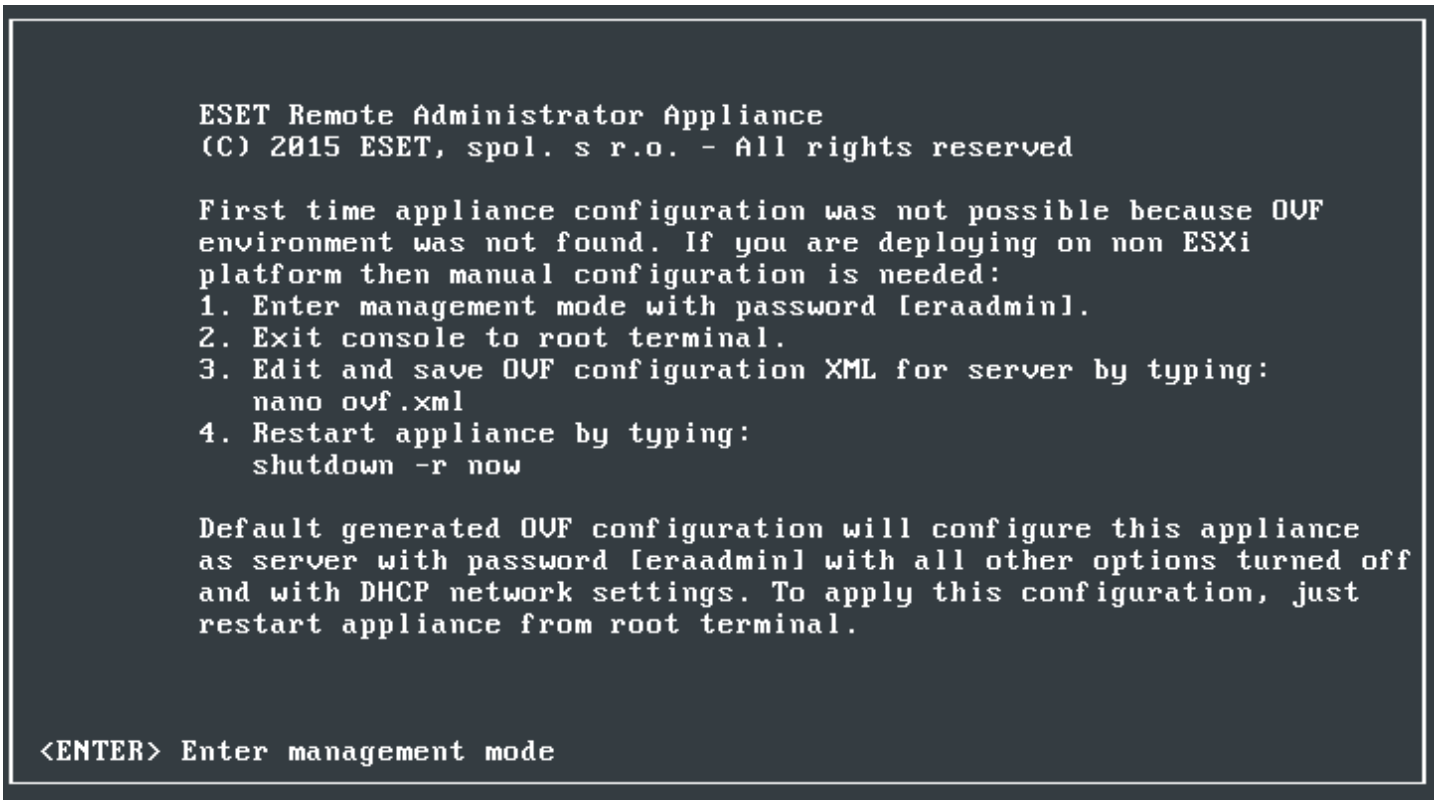
6. È necessario modificare il file di configurazione `ovf.xml` per inserire i dettagli relativi alla connessione del database e così via. Per eseguire questa operazione, seguire le istruzioni a schermo.

3.4.2 Oracle VirtualBox

Utilizzo di un file OVA in VirtualBox

Si consiglia di utilizzare la versione più recente di VirtualBox.

1. Fare clic su **File** e selezionare **Importa accessori...**
2. Fare clic su **Sfoglia** e accedere al file OVA (`ERA_Server.ova`) scaricato dal sito Web di ESET e fare clic su Apri. Fare clic su **Avanti**.
3. Rivedere le impostazioni degli accessori e fare clic su **Importa**.
4. Leggere e accettare eventualmente l'Accordo di licenza per l'utente finale (ALUF).
5. Dopo aver eseguito la distribuzione degli accessori, è possibile attivarli. Verranno visualizzate le seguenti informazioni:


ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved
First time appliance configuration was not possible because OVF environment was not found. If you are deploying on non ESXi platform then manual configuration is needed:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
nano ovf.xml
4. Restart appliance by typing:
shutdown -r now
Default generated OVF configuration will configure this appliance as server with password [eraadmin] with all other options turned off and with DHCP network settings. To apply this configuration, just restart appliance from root terminal.
<ENTER> Enter management mode

6. È necessario modificare il file di configurazione `ovf.xml` per inserire i dettagli relativi alla connessione del database e così via. Per eseguire questa operazione, seguire le istruzioni a schermo.

3.4.3 Microsoft Hyper-V

Utilizzo di un file OVA in Microsoft Hyper-V

1. Estrarre i file (scaricati dal sito Web di ESET) dal file degli accessori virtuali (`ERA_Server.ova`) utilizzando un'utilità come Tar o 7-Zip. Verranno visualizzati vari file estratti, tra cui il file `.vmdk` (ad esempio, `ERA_Server-disk1.vmdk`).
2. Scaricare e installare Microsoft Virtual Machine Converter 3.0 http://www.microsoft.com/en-us/download/details.aspx?id=42497.
3. Assicurarsi che sul sistema in uso sia disponibile Windows PowerShell 3.0 (o una versione successiva), specialmente su Windows 7. Per eseguire questa operazione, seguire le istruzioni sottostanti:
   a. aprire un prompt dei comandi Windows (**cmd.exe**).
   b. digitare `powershell`nel prompt dei comandi e premere Invio.
   c. In PowerShell, digitare `$PSVersionTable` e premere **Invio**.
   d. Se si visualizza **PSVersion 3.0** (o versioni successive), accedere al passaggio 5. In caso contrario, scaricare e installare Windows Management Framework 3.0 http://www.microsoft.com/en-us/download/details.aspx?id=34595.
   e. Ripetere i passaggi a-c per verificare che Powershell 3.0 o versioni successive sia installato e andare direttamente al passaggio 5.
4. Eseguire PowerShell e i comandi adottando la procedura sottostante.
5. Eseguire il comando del modulo di importazione:
   ```
   import-Module 'C:\Program Files\Microsoft Virtual Machine Converter\MvmcCmdlet.psd1'
   ```
6. Per confermare che l'importazione è stata eseguita in modo corretto, rivedere i moduli importati utilizzando il seguente comando:
   ```
   get-command -Module mvmccmdlet
   ```
7. Convertire il disco `.vmdk` che è stato estratto al passaggio 1. (`ERA_Server-disk1.vmdk` in caso di utilizzo del server ERA):

a. In Windows 7, è necessario utilizzare il **formato VHD**:
```
ConvertTo-MvmcVirtualHardDisk -SourceLiteralPath <path>\ERA_Server-disk1.vmdk -
DestinationLiteralPath <output-dir> -VhdType DynamicHardDisk -VhdFormat Vhd
```

b. In Windows 8 e versioni successive, è necessario utilizzare il **formato VHDX**:
```
ConvertTo-MvmcVirtualHardDisk -SourceLiteralPath <path>\ERA_Server-disk1.vmdk -
DestinationLiteralPath <output-dir> -VhdType DynamicHardDisk -VhdFormat Vhdx
```

8. Effettuare la connessione a Hyper-V.
9. Creare una nuova macchina virtuale (Generazione 1) con almeno 4 Core e 4 GB di RAM. Questa macchina virtuale utilizzerà il disco convertito nel passaggio 7.

3.5 Cluster di failover - Windows

I passaggi per utenti esperti necessari per installare ESET Remote Administrator in un ambiente con un cluster di failover sono i seguenti:

1. Creare un cluster di failover. È necessario un disco condiviso, un indirizzo IP e un nome cluster.
   a. Istruzioni per creare un cluster di failover in Windows Server 2012
   b. Istruzioni per creare un cluster di failover in Windows Server 2008
2. Installare il server ERA e l'agente ERA sul nodo attivo. Scegliere il disco condiviso come archiviazione dei dati applicativi.
3. Cambiare il nodo attivo e ripetere il passaggio 2.
4. Nella gestione configurazione del cluster creare 2 servizi cluster: agente ERA e server ERA.
5. Impostare le dipendenze appropriate: i servizi devono iniziare dopo che le risorse del passaggio 1 sono inizializzate. L'agente ERA deve inoltre essere dipendente dal server ERA.
6. Il database e il server Web non sono supportati su un cluster.

NOTA: non è possibile installare il server ERA su un cluster di failover tramite il programma di installazione ERA. Per installare ESET Remote Administrator su un cluster di failover, eseguire un'installazione dei componenti.

3.6 Cluster di failover - Linux

Di seguito viene illustrata la procedura di installazione e configurazione di ESET Remote Administrator su un cluster ad alta disponibilità Red Hat.

- Supporto cluster Linux
- Prerequisiti
- Ambito
- Passaggi dell'installazione

Supporto cluster Linux

I componenti del server ESET Remote Administrator o del proxy ERA possono essere installati sul cluster **Red Hat Linux 6** e versioni successive. Il cluster di failover è supportato solo in modalità attiva/passiva, con l'amministratore del cluster **rgmanager**.

Prerequisiti

- È necessario che sia installato e configurato il cluster attivo/passivo. Deve essere attivo un solo nodo alla volta. Gli altri nodi devono essere in standby. Non è supportato il bilanciamento del carico.

- Archiviazione condivisa: sono supportate le archiviazioni condivise iSCSI SAN, NFS e altre soluzioni (qualsiasi tecnologia o protocollo che consente l'accesso basato sui blocchi o sui file all'archiviazione condivisa e che faccia apparire i dispositivi condivisi come dispositivi collegati localmente al sistema operativo). L'archiviazione condivisa deve essere accessibile da ciascun nodo attivo nel cluster, mentre il sistema dei file condivisi deve essere correttamente inizializzato (ad esempio utilizzando il file system EXT3 o EXT4).
- Per la gestione del sistema sono richiesti i seguenti componenti aggiuntivi ad alta disponibilità:
  - rgmanager
  - Conga
- **rgmanager** è lo stack del cluster ad alta disponibilità Red Hat tradizionale. È un componente obbligatorio.
- L'interfaccia utente grafica (GUI) **Conga** è facoltativa. Il cluster di failover può essere gestito senza di essa. Per prestazioni ottimali è tuttavia consigliabile installarla. Nella presente guida si presuppone che sia installata.
- Per impedire il danneggiamento dei dati, è necessario che le **Fencing** siano configurate correttamente. È necessario che l'amministratore del cluster configuri le recinzioni, se non ancora configurate.

Se non è già in esecuzione un cluster, è possibile fare riferimento alla seguente guida per configurare un cluster di failover ad alta disponibilità (attivo/passivo) su Red Hat: Amministrazione cluster Red Hat Enterprise Linux 6.

Ambito

Componenti di ESET Remote Administrator che è possibile installare su un cluster ad alta disponibilità **Red Hat Linux**:

- Server ERA con agente ERA
- Proxy ERA con agente ERA

NOTA: è necessario che l'agente ERA sia installato. In caso contrario, il servizio del cluster ERA non verrà eseguito.

NOTA: l'installazione del database ERA o di ERA Web Console su un cluster non è supportata.

Il seguente esempio di installazione si riferisce a un cluster a 2 nodi. È tuttavia possibile installare ESET Remote Administrator su un cluster a nodi multipli utilizzando l'esempio a titolo di riferimento. I nodi del cluster nell'esempio fornito sono denominati nodo1 e nodo2.

Passaggi dell'installazione

1. Installare il server ERA o il proxy ERA, quindi l'agente ERA sul nodo1. Durante l'installazione dell'agente ERA, quando si utilizza il comando `--hostname=` è possibile specificare `localhost` (non utilizzare l'indirizzo IP o il nome host reale di tale nodo specifico). In alternativa, è possibile specificare l'indirizzo IP esterno o il nome host dell'interfaccia del cluster.

- Si tenga presente che il nome host nel certificato del server o del proxy deve contenere l'IP esterno (o nome host) dell'interfaccia del cluster (e non l'IP locale o il nome host del nodo).
- Durante l'installazione dell'agente ERA, quando si utilizza il comando --hostname=, sono disponibili le seguenti opzioni:
  - È possibile specificare l'indirizzo IP esterno o il nome host dell'interfaccia del cluster.
  - In alternativa, è possibile specificare il localhost (e non l'indirizzo IP o il nome host effettivo di quello specifico nodo). In questo caso, il nome host del certificato del server ERA o del proxy ERA deve contenere anche il localhost.

2. Interrompere e disabilitare i servizi Linux dell'agente ERA e del server ERA (o del proxy ERA) usando i seguenti comandi:

```
chkconfig eraagent off
chkconfig eraserver off
service eraagent stop
service eraserver stop
```

3. Montare l'archiviazione condivisa sul nodo1. Nell'esempio, l'archiviazione condivisa è montata su **/usr/share/erag2cluster**.

4. In **/usr/share/erag2cluster**, creare le seguenti directory:

/usr/share/erag2cluster/etc/opt
/usr/share/erag2cluster/opt
/usr/share/erag2cluster/var/log
/usr/share/erag2cluster/var/opt

5. Spostare in modo ricorsivo le seguenti directory nelle destinazioni riportate di seguito (origine > destinazione):

Spostare la cartella:	Spostare in:
/etc/opt/eset	/usr/share/erag2cluster/etc/opt/
/opt/eset	/usr/share/erag2cluster/opt/
/var/log/eset	/usr/share/erag2cluster/var/log/
/var/opt/eset	/usr/share/erag2cluster/var/opt/

6. Creare collegamenti simbolici:

ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset

7. Smontare l'archiviazione condivisa dal nodo1, montarla sulla stessa directory montata sul nodo1 (**/usr/share/erag2cluster**) sul nodo2.

8. Sul nodo2 creare i seguenti collegamenti simbolici:

ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset

9. Copiare lo script `eracluster_server` (`eracluster_proxy`) su **/usr/share/cluster**.

   Gli script `eracluster_server` (`eracluster_proxy`)) sono situati nella directory di configurazione del server ERA o del proxy ERA.

I passaggi successivi sono eseguiti nell'interfaccia grafica utente di Conga Cluster Administration:

10. Creare un gruppo di servizi, ad esempio EraService.

Il servizio del cluster ESET Remote Administrator richiede tre risorse: indirizzo IP, file system e script.

11. Creare le risorse del servizio necessarie.

    Aggiungere le risorse indirizzo IP, file system e script.
    La risorsa file system deve puntare all'archiviazione condivisa.
    Il punto di installazione della risorsa del file system deve essere impostato su **/usr/share/erag2cluster**.
    Il parametro "Full Path to Script File" della risorsa dello script deve essere impostato su **/usr/share/cluster/eracluster_server** (o **/usr/share/cluster/eracluster_proxy**)

12. Aggiungere le suddette risorse al gruppo EraService.

3.7 Installazione componenti su Windows

Nella maggior parte degli scenari di installazione, è necessario installare vari componenti ESET Remote Administrator su diverse macchine per adattare le varie architetture di rete, soddisfare requisiti in termini di prestazioni e così via. Per questo tipo di installazione, sono disponibili pacchetti di installazione per i singoli componenti.

Componenti principali

- Server ERA
- ERA Web Console
- Agente ERA (deve essere installato sui computer client, facoltativo sul server ERA)

Componenti facoltativi

- Proxy ERA
- Sensore RD
- Connettore dispositivi mobili
- Proxy Apache HTTP

Se si desidera aggiornare ESET Remote Administrator all'ultima versione (6.x), consultare questo articolo della Knowledge Base.

3.7.1 Installazione server - Windows

Per installare il componente Server ERA su Windows, adottare la procedura che segue:

1. Assicurarsi che vengano soddisfatti tutti i prerequisiti.
2. Eseguire il programma di installazione del server ERA e accettare l'EULA, se d'accordo.

NOTA: nel caso in cui si stia installando il server ERA su un cluster di failover, selezionare la casella di controllo accanto a **Questa è un'installazione cluster**. In caso contrario, lasciare vuota questa casella di controllo.

3. Se l'installazione viene eseguita su un cluster di failover, specificare il **Percorso personalizzato dati applicazioni** per puntare all'archiviazione condivisa del cluster. È necessario che i dati siano archiviati in una posizione che sia accessibile da tutti i nodi all'interno del cluster.
4. Inserire una Chiave di licenza ERA valida o scegliere **Attiva in seguito**.
5. Selezionare un **Account utente di servizio**. Questo account verrà utilizzato per eseguire il servizio del server ESET Remote Administrator. Sono disponibili le seguenti opzioni:
    - Account servizio di rete
    - Utente specificato: DOMINIO/NOME UTENTE
4. Effettuare la connessione a un database. Tutti i dati vengono memorizzati qui (password di ERA Web Console, rapporti dei computer client, ecc.):
    - **Database**: MySQL Server/MS SQL Server/MS SQL Server tramite autenticazione di Windows
    - **Driver ODBC**: Driver MySQL ODBC 5.1/Driver MySQL ODBC 5.2 Unicode/Driver MySQL ODBC 5.3 Unicode/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 per SQL Server
    - **Nome database**: è possibile lasciare il nome predefinito o modificarlo, se necessario
    - **Nome host**: nome host o indirizzo IP del server del database
    - **Porta:** utilizzata per la connessione al server del database
    - **Nome utente**/**Password** dell'account amministratore database

NOTA: il server ERA memorizza enormi quantità di blob di dati nel database. Di conseguenza, è necessario configurare MySQL per accettare pacchetti di grandi dimensioni che garantiscano un corretto funzionamento di ERA. Per ulteriori informazioni sulle modalità di configurazione di questa funzione, consultare le Domande frequenti.

Questo passaggio consentirà di verificare la connessione al database. Se la connessione è corretta, è possibile procedere al passaggio successivo.

5. Selezionare un utente per ESET Remote Administrator che ha accesso al database. È possibile utilizzare un utente esistente oppure ne verrà creato uno dalla configurazione.
6. Inserire una password per l'accesso alla **Console Web**.
7. ESET Remote Administrator utilizza certificati per la comunicazione client-server. È possibile selezionare i propri certificati oppure i certificati creati dal **Server**.
8. Inserire la password per l'**Autorità di certificazione**. facendo attenzione a non dimenticarla.
9. Verrà creato un nuovo server di certificazione, per il quale dovrà essere selezionata una password.
10. Nel passaggio successivo, selezionare una password per il certificato dell'**Agente**.

La configurazione può eseguire un'attività di Sincronizzazione di gruppi statici iniziale. Selezionare il metodo (**Non sincronizzare**, **Sincronizza con la rete Windows**, **Sincronizza con Active Directory**) e fare clic su **Avanti**.

Confermare o modificare la cartella di installazione per il server e fare clic su **Avanti**.

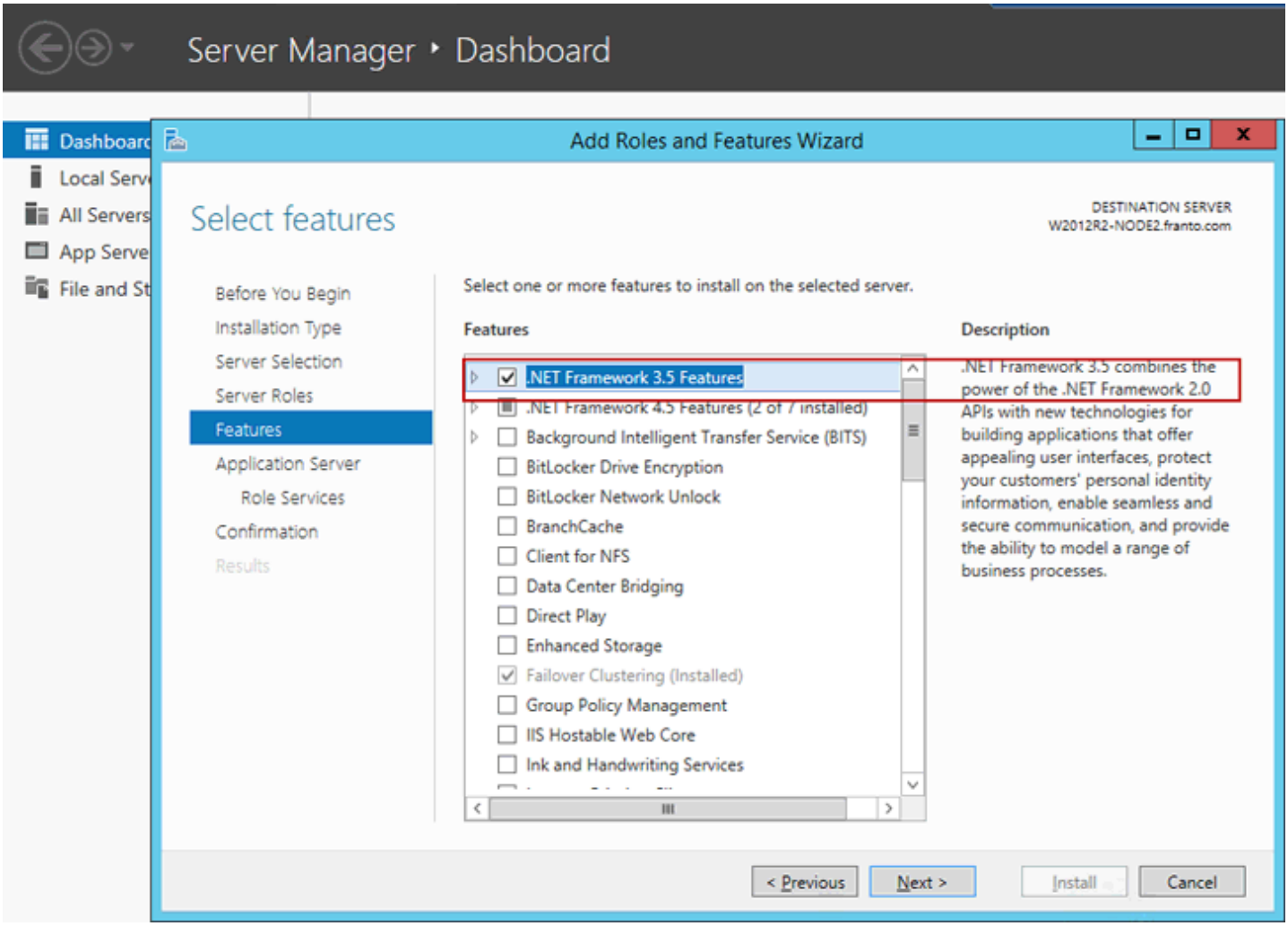
Fare clic su **Installa** per installare il server.

NOTA: al termine dell'installazione del server ERA, è possibile installare anche l'agente ERA sulla stessa macchina (facoltativo). In tal modo, sarà possibile gestire il server allo stesso modo di un computer client.

3.7.1.1 Prerequisiti server - Windows

Per installare il server ERA su Windows, è necessario che vengano soddisfatti i seguenti prerequisiti:

- È necessario disporre di una licenza valida.
- Le porte richieste devono essere aperte e disponibili: per un elenco completo delle porte, fare clic qui.
- Server del database (Microsoft SQL Server o MySQL) installato e in esecuzione. Per ulteriori informazioni, consultare requisiti del database. Se non si è in possesso di un server del database esistente, si consiglia di revisionare i dettagli della Configurazione di SQL Server per configurare correttamente SQL ai fini dell'utilizzo con ESET Remote Administrator.
- Java Runtime Environment (JRE) deve essere installato (è possibile scaricarlo da http://java.com/en/download/), utilizzare sempre l'ultima versione di Java rilasciata ufficialmente.
- È necessario che sia installato Microsoft .NET Framework 3.5. Se si esegue Windows Server 2008 o 2012, è possibile installarlo tramite la **Procedura guidata regole e funzioni** (come mostrato di seguito), mentre se si utilizza Windows Server 2003, è possibile scaricare .NET 3.5 all'indirizzo http://www.microsoft.com/en-us/download/details.aspx?id=21


Server Manager ‣ Dashboard
Add Roles and Features Wizard
Select features
DESTINATION SERVER
W2012R2-NODE2.franto.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Application Server
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
Description
.NET Framework 3.5 Features
.NET Framework 4.5 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering (Installed)
Group Policy Management
IIS Hostable Web Core
Ink and Handwriting Services
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

NOTA: se si sceglie di installare Microsoft SQL Server Express durante l'installazione di ESET Remote Administrator, non sarà possibile istallarlo su un controller di dominio. Ciò si verificherà molto probabilmente se si utilizza Microsoft SBS. Se si utilizza Microsoft SBS, è consigliabile installare ESET Remote Administrator su un server differente o non selezionare il componente SQL Server Express durante l'installazione (poiché richiede l'utilizzo di un SQL Server o MySQL esistente per l'esecuzione del database ERA). Per consultare le istruzioni per l'installazione del server ERA su un controller di dominio, leggere questo articolo della Knowledge Base.

NOTA: il server ERA memorizza enormi quantità di blob di dati nel database. Di conseguenza, è necessario configurare MySQL per accettare pacchetti di grandi dimensioni che garantiscano un corretto funzionamento di ERA. Per ulteriori informazioni su questa modifica, consultare le Domande frequenti.

3.7.2 Microsoft SQL Server - Windows

Uno dei prerequisiti dell'installazione del server ERA consiste nell'installazione e nella configurazione di Microsoft SQL Server ai fini dell'utilizzo con ESET Remote Administrator. È necessario che vengano soddisfatti i seguenti requisiti:

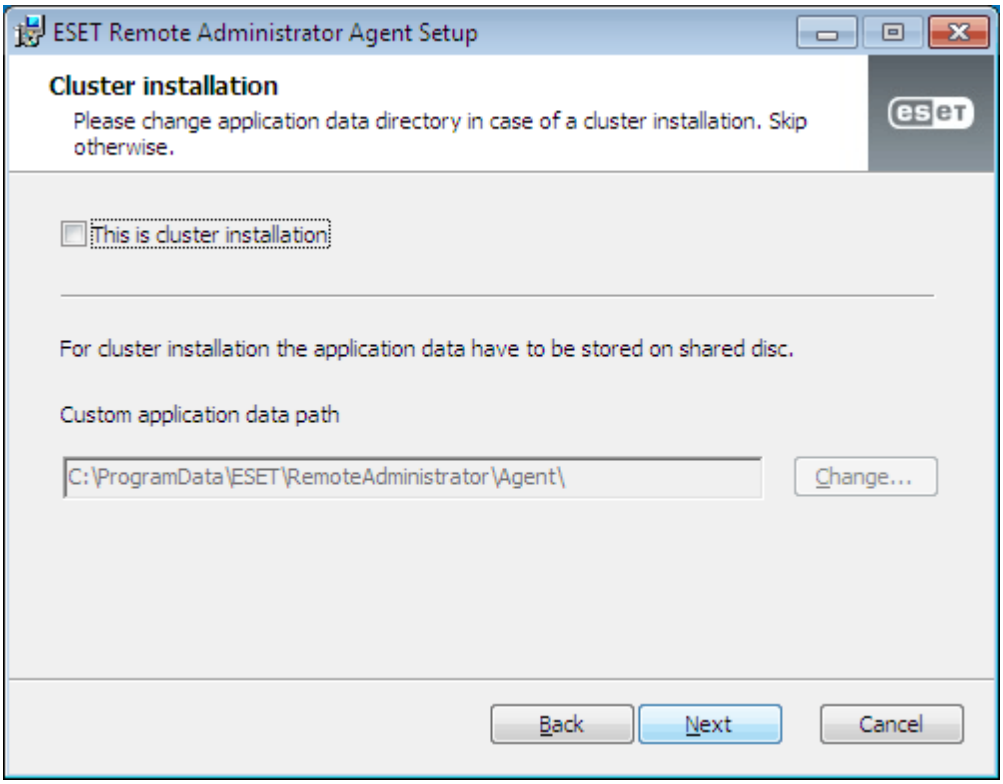
- Installare Microsoft SQL Server 2008 R2 o versioni successive e, in alternativa, Microsoft SQL Server 2008 R2 Express o versioni successive. Scegliere l'autenticazione **Modalità mista** durante l'installazione.
- Se Microsoft SQL Server è già stato installato, impostare l'autenticazione su **Modalità mista (autenticazione di SQL Server e autenticazione di Windows)**. Per eseguire questa operazione, seguire le istruzioni contenute in questo articolo della Knowledge Base.
- Consentire le connessioni TCP/IP a SQL Server. Per eseguire questa operazione, seguire le istruzioni contenute in questo articolo della Knowledge Base a partire dalla sezione **II. Consentire le connessioni TCP/IP al database SQL**.

3.7.3 Installazione dell'agente - Windows

Per installare il componente Agente ERA su Windows, adottare la procedura che segue:

1. Eseguire il programma di installazione dell'agente ERA e accettare l'EULA, se d'accordo.

NOTA: nel caso in cui si stia installando l'agente ERA su un cluster di failover, selezionare la casella di controllo accanto a **Questa è un'installazione cluster**. In caso contrario, lasciare vuota questa casella di controllo.



2. Se l'installazione viene eseguita su un cluster di failover, specificare il **Percorso personalizzato dati applicazioni** per puntare all'archiviazione condivisa del cluster. È necessario che i dati siano archiviati in una posizione che sia accessibile per tutti i nodi all'interno del cluster.
3. Immettere l'**Host del server** (nome o indirizzo IP del server ERA) e la **Porta server** (la porta predefinita è 2222. Se si utilizza una porta differente, sostituire quella predefinita con il numero di porta personalizzato).

Selezionare una delle seguenti opzioni di installazione e attenersi ai passaggi relativi alla sezione appropriata qui di seguito:

- **Installazione assistita dal server**: sarà necessario fornire le credenziali amministratore di ERA Web Console (i certificati richiesti saranno scaricati automaticamente).
- **Installazione off-line**: sarà necessario fornire un **Certificato dell'agente**che può essere esportato da ESET Remote Administrator. In alternativa, è possibile utilizzare il proprio certificato personalizzato.

Installazione assistita dal server:

4. Immettere l'**Host del server** (nome o indirizzo IP del server ERA) e la **Porta console Web** (lasciare la porta predefinita 2223 se non si utilizza una porta personalizzata). Fornire inoltre le credenziali dell'account amministratore della console Web (**Nome utente**/**Password**).
5. Se si desidera accettare il certificato, fare clic su Sì quando richiesto.
6. Scegliere **Non creare computer** o **Scegli gruppo statico personalizzato**. Se si seleziona **Scegli gruppo statico personalizzato** sarà possibile scegliere da un elenco di Gruppi statici esistenti in ERA. Il computer verrà aggiunto al gruppo selezionato dall'utente.
7. Specificare una cartella di destinazione per l'agente ERA (si consiglia di utilizzare il percorso predefinito), fare clic su **Avanti**, quindi su **Installa**.

Installazione off-line:

4. Fare clic su **Sfoglia** e accedere al percorso del certificato del peer (ovvero il certificato dell'agente esportato da ERA). Lasciare vuoto il campo di testo **Password del certificato** poiché questo certificato non richiede una password. Non è necessario ricercare un'**Autorità di certificazione** (lasciare questo campo vuoto).

NOTA: se si utilizza un certificato personalizzato con ERA (anziché quelli predefiniti generati automaticamente durante l'installazione di ESET Remote Administrator), utilizzare i certificati personalizzati.

5. Fare clic su **Avanti** per eseguire l'installazione sulla cartella predefinita oppure fare clic su **Cambia** per scegliere un'altra cartella (si consiglia di utilizzare il percorso predefinito).

3.7.4 Installazione console Web - Windows

Per installare il componente ERA Web Console su Windows, seguire la procedura sottostante:

1. Verificare che vengano soddisfatti i seguenti prerequisiti:
   - Java: utilizzare sempre l'ultima versione di Java rilasciata ufficialmente (ERA Web Console richiede come requisito minimo Java versione 7, ma si consiglia vivamente di utilizzare l'ultima versione).
   - Apache Tomcat (versione 6 o successive).
   - File della console Web (*era.war*) salvato sul disco rigido locale.
2. Copiare *era.war* nella cartella delle applicazioni Web Tomcat (sulla maggior parte dei sistemi operativi: *C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\).*
3. Riavviare il servizio *Apache Tomcat*.
4. Aprire https://localhost/era/ nel browser in uso su localhost. A questo punto, verrà visualizzata una schermata di accesso.

3.7.4.1 Browser Web supportati

Browser Web	Versione
Mozilla Firefox	20+
Internet Explorer	10+
Chrome	23+
Safari	6+
Opera	12+

3.7.5 Installazione proxy - Windows

Per installare il componente ERA Proxy Server su Windows, seguire la procedura sottostante:

1. Assicurarsi che vengano soddisfatti tutti i prerequisiti.

NOTA: nel caso in cui si stia installando il server del proxy ERA su un cluster di failover, selezionare la casella di controllo **Questa è un'installazione cluster**. In caso contrario, lasciare vuota questa casella di controllo.

2. Se l'installazione viene eseguita su un cluster di failover, specificare il **Percorso personalizzato dati applicazioni** per puntare a un'archiviazione condivisa del cluster. È necessario che i dati siano archiviati in una posizione che sia accessibile da tutti i nodi all'interno del cluster.

3. Selezionare un account utente di servizio. Questo account verrà utilizzato per eseguire il servizio del server ESET Remote Administrator. Sono disponibili le seguenti opzioni:

   a. Account servizio di rete
   b. Account personalizzato: DOMINIO/NOME UTENTE

4. Effettuare la connessione a un database. Tutti i dati vengono memorizzati qui, dalla password di ERA Web Console ai rapporti dei computer client.

   a. Database: MySQL/MS SQL
   b. Driver ODBC: Driver MySQL ODBC 5.1/MySQL ODBC 5.2 ANSI/Server DriverSQL
   c. Nome host del server del database
   d. Porta utilizzata per la connessione con il server
   e. Nome database
   f. Accesso/password amministratore DB
   g. Accesso/password utente database ERA

Questo passaggio consentirà di verificare la connessione al database. Se la connessione è corretta, è possibile procedere al **passaggio** successivo. Se non è possibile stabilire una connessione, verrà visualizzato un messaggio di errore.

4. Selezionare una porta di comunicazione del proxy. Per impostazione predefinita, verrà utilizzata la porta 2222.

5. Configurare la connessione del proxy a ESET Remote Administrator. Inserire un **Host del server** (nome host/ indirizzo IP del server) e la **Porta del server** (2222).

6. Selezionare un certificato del peer e una password per il certificato. Facoltativamente, è anche possibile aggiungere un'autorità di certificazione. Questo valore deve essere inserito necessariamente solo per i certificati privi di firma.

7. Selezionare una cartella in cui verrà installato il **Proxy** oppure lasciare selezionata la cartella predefinita.

8. Fare clic su **Installa**. Il **Proxy** verrà installato sul computer in uso.

NOTA: durante l'installazione del proxy ERA, l'installazione assistita dal server non è supportata.

3.7.5.1 Prerequisiti proxy - Windows

Per installare il componente ERA Proxy Server su Windows, è necessario che vengano soddisfatti i seguenti prerequisiti:

- Il **Server ERA** ed **ERA Web Console** sono installati (su un computer server).
- Il **Certificato del proxy** è stato creato e scaricato sull'unità locale.
- È stata preparata l'**Autorità di certificazione** sull'unità locale.
- Una licenza valida.
- Un server del database già installato e configurato.
- Un driver ODBC per la connessione al server del database (MySQL/MS SQL) installato sul computer.
- Per poter supportare tutte le funzioni del programma, l'agente deve essere installato su un computer locale.

3.7.6 Installazione RD Sensor - Windows

Per installare il componente RD Sensor su Windows, adottare la procedura che segue:

1. Assicurarsi che vengano soddisfatti tutti i prerequisiti.
2. Fare doppio clic sul file del programma di installazione di RD Sensor per avviare l'installazione.
3. Selezionare il punto in cui RD Sensor verrà installato e fare clic su **Avanti** > **Installa**.

3.7.6.1 Prerequisiti RD Sensor - Windows

Per installare il componente RD Sensor su Windows, è necessario che vengano soddisfatti i seguenti prerequisiti:

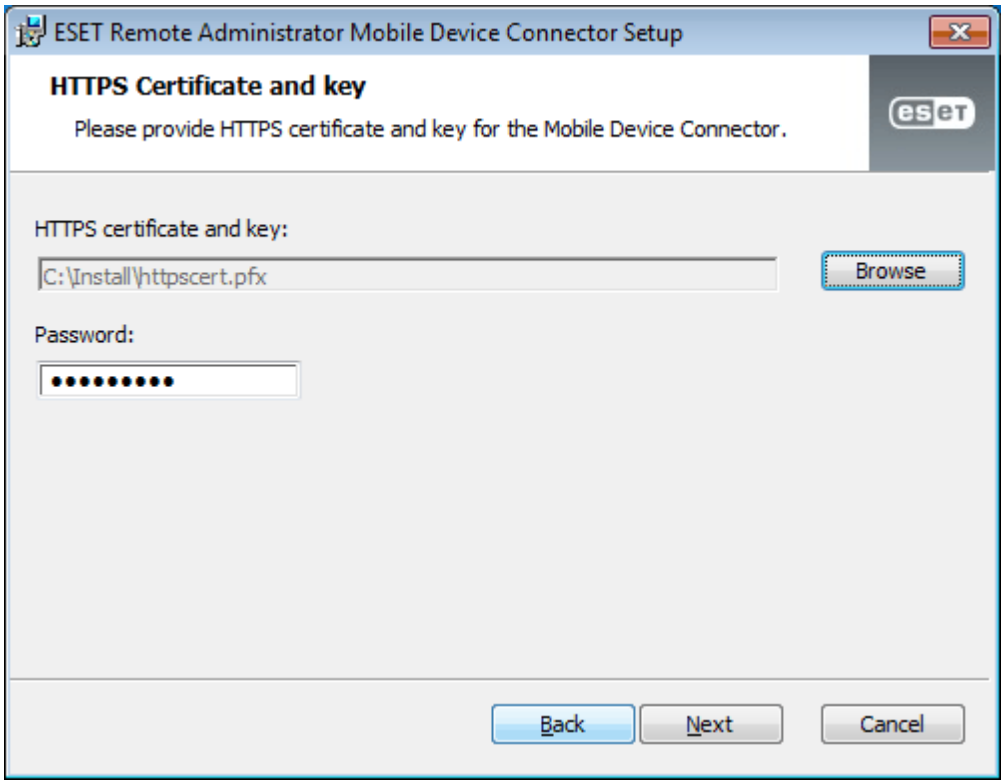
- WinPcap: utilizzare l'ultima versione di WinPcap (versione minima: 4.1.0)
- È necessario configurare correttamente la rete (porte appropriate aperte, comunicazioni in entrata non bloccate da un Firewall, ecc.)
- Server ERA raggiungibile
- Per poter supportare tutte le funzioni del programma, l'Agente ERA deve essere installato sul computer locale
- Il file di rapporto di Rogue Detection Sensor è disponibile qui: *C:\ProgramData\ESET\Rouge Detection Sensor \Logs\trace.log*

3.7.7 Installazione di Connettore dispositivi mobili - Windows

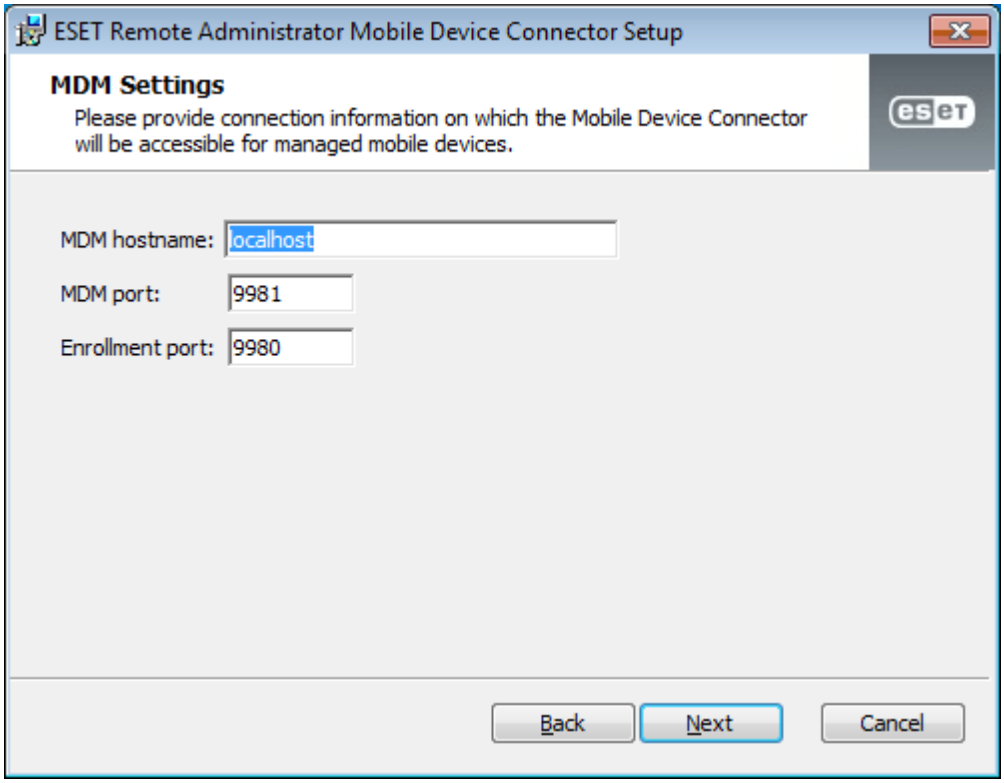
Il componente Connettore dispositivi mobili può essere installato su un server differente da quello in cui è in esecuzione il server ERA. Ad esempio, se si desidera rendere Connettore dispositivi mobili accessibile da Internet in modo da poter gestire i dispositivi mobili dell'utente in qualsiasi momento, indipendentemente dalla rispettiva posizione.

Per installare Connettore dispositivi mobili su Windows attenersi ai passaggi illustrati di seguito:

1. Assicurarsi che vengano soddisfatti tutti i prerequisiti.
2. Eseguire il programma di installazione Connettore dispositivi mobili e accettare l'EULA, se d'accordo.
3. Fare clic su **Sfoglia**, accedere alla posizione del Certificato SSL per la comunicazione tramite HTTPS e immettere la password per questo certificato:



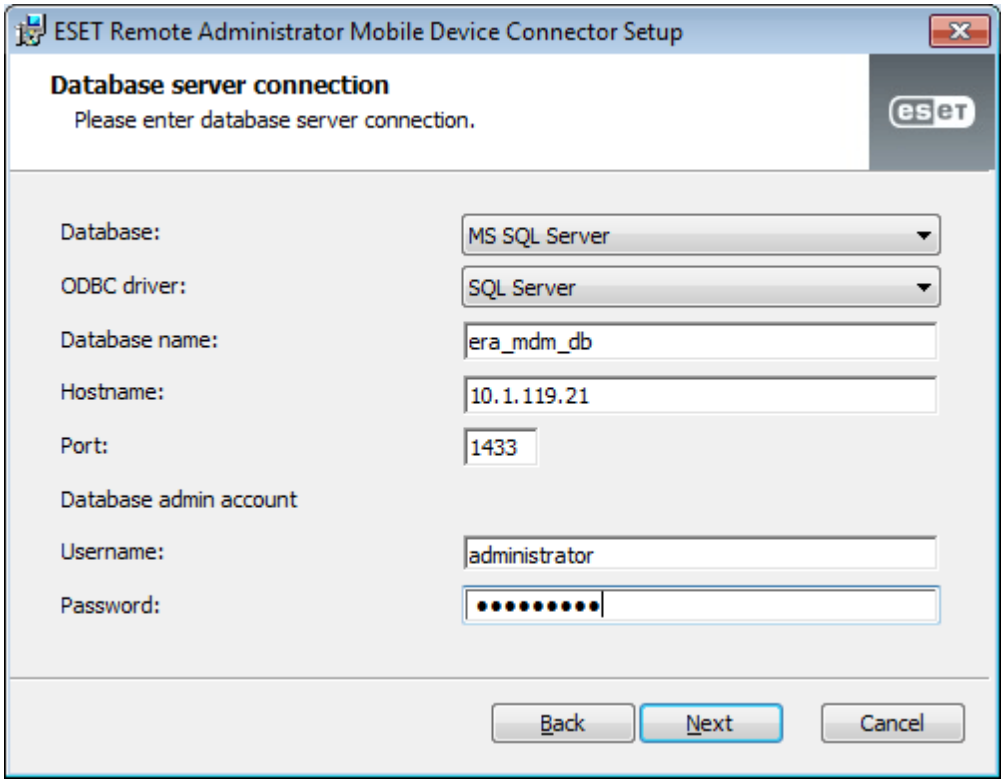
4. Si consiglia di utilizzare il nome host e le porte predefiniti (9981 e 9980). È tuttavia possibile specificare le porte desiderate, se necessario. Assicurarsi che i dispositivi riescano a connettersi tramite queste due porte sul server sul quale si sta installando Connettore dispositivi mobili. Modificare le impostazioni del firewall (se applicabile) per consentire di eseguire questa operazione.



5. Sarà necessario creare un nuovo database che sarà utilizzato da Connettore dispositivi mobili. Pertanto, fornire i dettagli della connessione:

- **Database**: MySQL Server/MS SQL Server/MS SQL Server tramite autenticazione di Windows
- **Driver ODBC**: Driver MySQL ODBC 5.1/Driver MySQL ODBC 5.2 Unicode/Driver MySQL ODBC 5.3 Unicode/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 per SQL Server
- **Nome database**: è possibile lasciare il nome predefinito o modificarlo, se necessario
- **Nome host**: nome host o indirizzo IP del server del database
- **Porta:** utilizzata per la connessione al server del database
- **Nome utente**/**Password** dell'account amministratore database

NOTA: è consigliabile utilizzare lo stesso server del database che si utilizza per il database ERA, anche se può essere un server del database differente, se necessario. Fare clic sul pulsante Avanti. Il programma di installazione di Connettore dispositivi mobili creerà il proprio database.



6. Specificare l'utente per il database del Connettore dispositivi mobili appena creato. È possibile scegliere l'opzione **Crea nuovo utente** o **Utilizza utente database esistente**. Immettere la password per l'utente del database.

7. Immettere l'**Host del server** (nome o indirizzo IP del server ERA) e la **Porta server** (la porta predefinita è 2222. Se si utilizza una porta differente, sostituire quella predefinita con il numero di porta personalizzato).

Sono ora disponibili due opzioni per proseguire con l'installazione:

- **Installazione assistita dal server**: sarà necessario fornire le credenziali amministratore di ERA Web Console (i certificati richiesti saranno scaricati automaticamente).
- **Installazione off-line**: sarà necessario fornire il **Certificato dell'agente**che può essere esportato da ESET Remote Administrator. In alternativa, è possibile utilizzare il proprio certificato personalizzato.

I seguenti passaggi sono applicabili se si seleziona **Installazione assistita dal server**:

8. Immettere l'**Host del server** (nome o indirizzo IP del server ERA) e la **Porta console Web** (lasciare la porta predefinita 2223 se non si utilizza una porta personalizzata). Fornire inoltre le credenziali dell'account amministratore della console Web (**Nome utente**/**Password**).

9. Quando viene visualizzato **Accetta certificato**, fare clic su **Sì**.

10. Specificare la cartella di destinazione per Connettore dispositivi mobili (si consiglia di utilizzare il percorso predefinito), fare clic su **Avanti**, quindi su **Installa**.

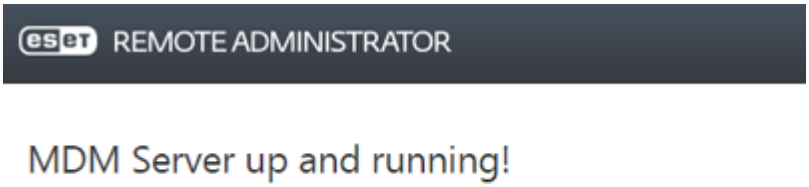
I seguenti passaggi sono applicabili se si seleziona **Installazione off-line**:

8. Fare clic su **Sfoglia** e accedere al percorso del certificato del peer (ovvero il certificato dell'agente esportato da ERA). Lasciare vuoto il campo di testo **Password del certificato** poiché questo certificato non richiede la password.

NOTA: se si utilizzano certificati personalizzati con ERA (anziché quelli predefiniti generati automaticamente durante l'installazione di ESET Remote Administrator), utilizzare i certificati personalizzati.

9. Fare clic su **Avanti** per eseguire l'installazione sulla cartella predefinita oppure fare clic su **Cambia...** per scegliere un'altra cartella (si consiglia di utilizzare il percorso predefinito).

Al termine dell'installazione, verificare la corretta esecuzione di Connettore dispositivi mobili aprendo https://*your-mdm-hostname*:*enrollment-port* (ad esempio https://eramdm:9980) nel browser Web. Se l'installazione è stata eseguita correttamente, verrà visualizzato il seguente messaggio:



È anche possibile utilizzare questo URL per verificare la disponibilità del server Connettore dispositivi mobili da Internet (se configurato in tal modo), ad esempio visitandolo da un dispositivo mobile. Se non si riesce a visualizzare la pagina, potrebbe essere necessario controllare il firewall e altri parametri di configurazione dell'infrastruttura di rete.

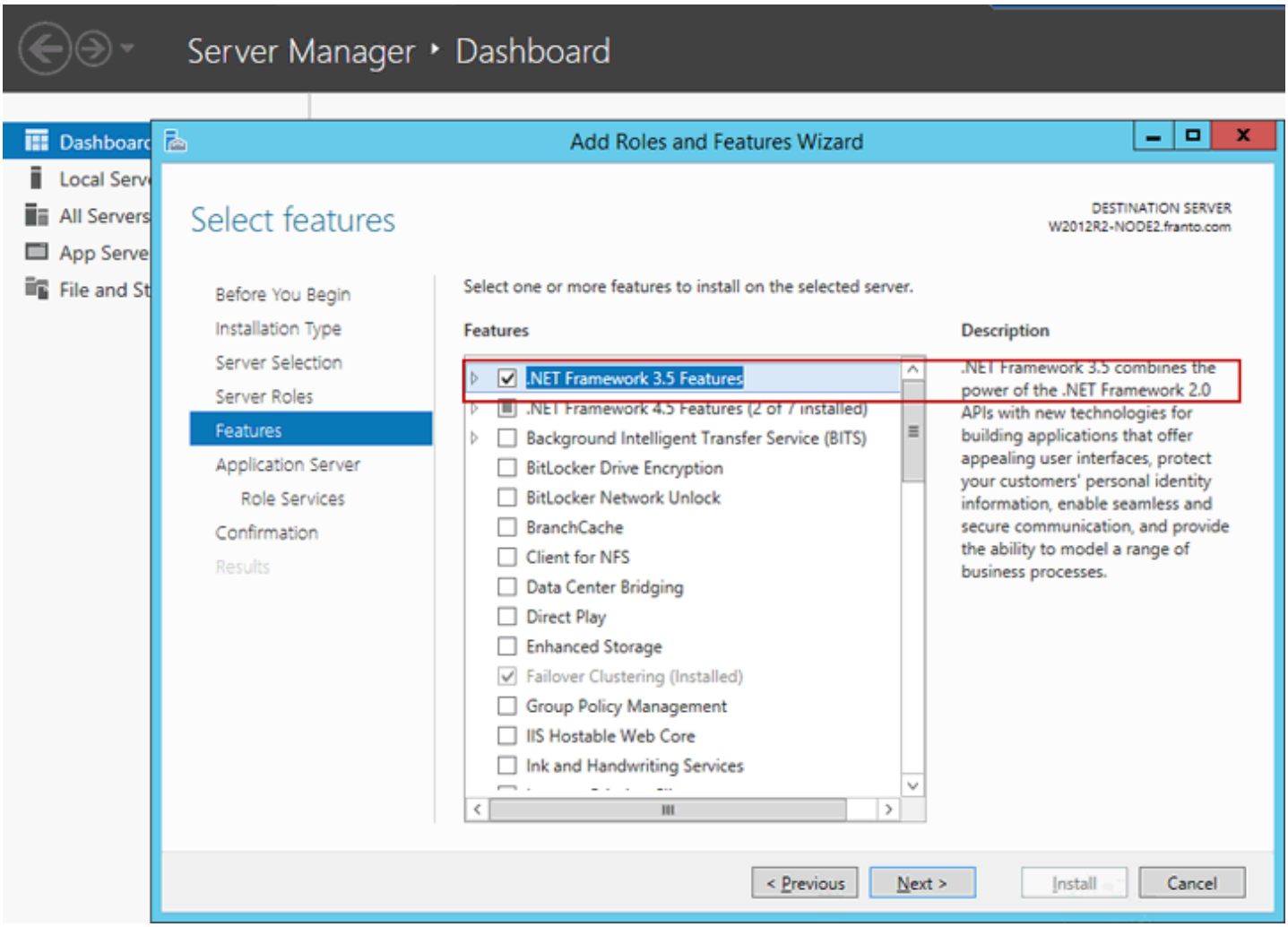
3.7.7.1 Prerequisiti di Connettore dispositivi mobili - Windows

Per installare Connettore dispositivi mobili su Windows, è necessario che vengano soddisfatti i seguenti prerequisiti:

- Porte aperte e disponibili: per un elenco completo delle porte, fare clic qui.
- Impostazioni firewall: in caso di installazione del Connettore dispositivi mobili su un sistema operativo non server, come ad esempio Windows 7 (solo per scopo di valutazione), assicurarsi di consentire le porte di comunicazione attraverso la creazione di regole firewall per:
  C:\Programmi\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, porta TCP 9980
  C:\Programmi\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, porta TCP 9981
  C:\Programmi\ESET\RemoteAdministrator\Server\ERAServer.exe, porta TCP 2222
  C:\Programmi\Apache HTTP Proxy\bin\httpd.exe, porta TCP 3128

  NOTA: i percorsi effettivi ai file .exe possono variare in base alla posizione in cui ciascuno dei componenti ERA è installato sul sistema operativo client dell'utente.
- Java Runtime Environment (JRE) deve essere installato (è possibile scaricarlo da http://java.com/en/download/), utilizzare sempre l'ultima versione di Java rilasciata ufficialmente.

- È necessario che sia installato Microsoft .NET Framework 3.5. Se si esegue Windows Server 2008 o 2012, è possibile installarlo tramite la **Procedura guidata regole e funzioni** (come mostrato di seguito), mentre se si utilizza Windows Server 2003, è possibile scaricare .NET 3.5 all'indirizzo http://www.microsoft.com/en-us/download/details.aspx?id=21


Server Manager ‣ Dashboard
Add Roles and Features Wizard
Select features
DESTINATION SERVER
W2012R2-NODE2.franto.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Application Server
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
Description
.NET Framework 3.5 Features
.NET Framework 4.5 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering (Installed)
Group Policy Management
IIS Hostable Web Core
Ink and Handwriting Services
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

NOTA: se si sceglie di installare Microsoft SQL Server Express durante l'installazione di ESET Remote Administrator, non sarà possibile istallarlo su un controller di dominio. Ciò si verificherà molto probabilmente se si utilizza Microsoft SBS. Se si utilizza Microsoft SBS, è consigliabile installare ESET Remote Administrator su un server differente o non selezionare il componente SQL Server Express durante l'installazione (poiché richiede l'utilizzo di un SQL Server o MySQL esistente per l'esecuzione del database ERA).

NOTA: il server ERA memorizza enormi quantità di blob di dati nel database. Di conseguenza, è necessario configurare MySQL per accettare pacchetti di grandi dimensioni che garantiscano un corretto funzionamento di ERA. Per ulteriori informazioni su questa modifica, consultare le Domande frequenti.

IMPORTANTE: sarà necessario un **certificato SSL** in formato `PFX` per comunicazioni sicure su HTTPS. Si consiglia l'utilizzo del certificato fornito dall'autorità di certificazione. L'uso dei certificati autofirmati è sconsigliato poiché non tutti i dispositivi mobili consentono agli utenti di accettare certificati autofirmati. Questo problema non si verifica con i certificati firmati da un'autorità di certificazione poiché sono attendibili e non richiedono l'accettazione da parte dell'utente.

IMPORTANTE: in caso di Installazione off-line sarà necessario fornire anche un **Certificato dell'agente**esportato da ESET Remote Administrator. In alternativa, è possibile utilizzare il proprio certificato personalizzato con ERA.

3.7.8 Installazione del proxy Apache HTTP - Windows

Il proxy Apache HTTP è un servizio che può essere utilizzato in combinazione con ESET Remote Administrator 6 e versioni successive ai fini della distribuzione degli aggiornamenti ai computer client e dei pacchetti di installazione all'agente ERA. Il proxy HTTP svolge un ruolo simile a quello del server mirror in ESET Remote Administrator 5 e nelle versioni precedenti. L'utilizzo del proxy HTTP offre i seguenti vantaggi:

- Download dei nuovi aggiornamenti del database delle firme antivirali e degli aggiornamenti dei componenti del prodotto e distribuzione di queste risorse ai client presenti nella rete.
- Creazione della cache relativa ai pacchetti di installazione del prodotto ESET.
- Riduzione al minimo del traffico Internet sulla rete in uso.

Per installare il componente proxy Apache HTTP su Windows, attenersi alla procedura che segue:

1. Aprire ApacheHttp.zip ed estrarre i file in *C:\Program Files\Apache HTTP Proxy*
2. Aprire un prompt dei comandi amministrativo e il CD in *C:\Program Files\Apache HTTP Proxy\bin*
3. Eseguire il seguente comando:

```
httpd.exe -k install -n ApacheHttpProxy
```

4. Utilizzando un editor di testo come Notepad, aprire il file httpd.conf e aggiungere le seguenti righe in fondo al file:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

5. Impostare il servizio del proxy Apache HTTP utilizzando il seguente comando:

```
sc start ApacheHttpProxy
```

6. È possibile verificare che il servizio del proxy Apache HTTP sia in esecuzione nello snap-in services.msc (ricercare ApacheHttpProxy). Per impostazione predefinita, il servizio è configurato per avviarsi automaticamente.

Attenersi ai seguenti passaggi per configurare un nome utente e una password per il proxy Apache HTTP (scelta consigliata):

1. Verificare la presenza dei seguenti moduli in *Apache HTTP Proxy\conf\httpd.conf*:

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

2. Aggiungere le seguenti righe a *Apache HTTP Proxy\conf\httpd.conf* sotto a `<Proxy *>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

3. Utilizzare il comando `htpasswd` per creare un file denominato `password.file` nella cartella *Apache HTTP Proxy\bin* \ (all'utente verrà richiesto di immettere la password):

```
htpasswd.exe -c ..\password.file username
```

4. Creare manualmente il file `group.file` nella cartella *Apache HTTP Proxy* con il seguente contenuto:

```
usergroup:username
```

5. Testare la connessione al proxy HTTP accedendo al seguente URL nel browser:

   http://localhost:3128/index.html

Utilizzare lo strumento htcacheclean per pulire la cache del disco. Questo strumento può essere eseguito sia manualmente sia in modalità daemon. Specificare il limite massimo delle dimensioni della cache totale sul disco. Per impostazione predefinita, il valore è espresso in byte (oppure in un numero seguito da B). Aggiungere K per Kbyte o M per MByte.

Per ulteriori informazioni, consultare questo articolo della Knowledge Base o la documentazione sull'autenticazione e l'autorizzazione dell'Apache.

3.8 Installazione componenti su Linux

Nella maggior parte degli scenari di installazione, è necessario installare vari componenti ESET Remote Administrator su diverse macchine per adattare le varie architetture di rete, soddisfare requisiti in termini di prestazioni e così via.

Componenti principali

- Server ERA
- ERA Web Console
- Agente ERA

Componenti facoltativi

- Proxy ERA
- Sensore RD
- Connettore dispositivi mobili
- Proxy Apache HTTP

Se si desidera aggiornare ESET Remote Administrator all'ultima versione (6.x), consultare questo articolo della Knowledge Base.

3.8.1 Installazione server - Linux

L'installazione del componente Server ERA su Linux viene eseguita attraverso un comando nel terminale. Assicurarsi che vengano soddisfatti tutti i prerequisiti. È possibile preparare uno script di installazione ed eseguirlo utilizzando il comando *sudo*.

Esempio
(Le nuove righe vengono separate da "\" per la copia dell'intero comando sul terminale)

```
sudo ./Server-Linux-i386.sh \
--skip-license \
--db-driver=MySQL \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=Admin123 \
--server-root-password=Admin123 \
--db-user-username=root \
--db-user-password=Admin123 \
--cert-hostname="10.1.179.46;Ubuntu64-bb;Ubuntu64-bb.BB.LOCAL"
```

Il server ERA e il servizio `eraserver` verranno installati nella seguente posizione:
/opt/eset/RemoteAdministrator/Server

È possibile modificare i seguenti attributi:

Attributo	Descrizione	Richiesto
--uninstall	Disinstalla il prodotto	-

Attributo	Descrizione	Richiesto
--locale	Identificatore delle impostazioni locali (LCID) del server installato (l'impostazione predefinita è "en_US"). Per visualizzare le opzioni disponibili, consultare la sezione lingue supportate. **Nota:** è possibile impostare una lingua per ciascuna sessione di ERA Web Console.	Sì
--skip-license	L'installazione non chiederà all'utente la conferma dell'accordo di licenza	
--skip-cert	Salta la generazione di certificati (utilizzare questa opzione insieme al parametro --percorso-cert-server)	
--license-key	Chiave di licenza ESET. Questa opzione può essere impostata in un momento successivo.	No
--product-guid	Identificatore globale univoco del prodotto. Se non impostato, questo valore verrà generato.	No
--server-port	Porta del server ESET Remote Administrator (ERA) (impostazione predefinita: 2222)	No
--console-port	Porta della console di ESET Remote Administrator (impostazione predefinita: 2223)	No
--server-root-password	Password per l'accesso alla console Web dell'utente "Amministratore", lunghezza minima 8 caratteri	Sì
--db-type	Tipo di database che verrà utilizzato (valori possibili: "MySQL Server", "Microsoft SQL Server")	
--db-driver	Driver ODBC utilizzato per la connessione al database (ad esempio, "Driver MySQL ODBC 5.3 ANSI")	Sì
--db-hostname	Nome del computer o indirizzo IP del server del database	Sì
--db-port	Porta del server del database (impostazione predefinita: 3306)	Sì
--db-nome	Nome del database del server ERA (impostazione predefinita: "era_db")	Sì
--db-admin-username	Nome utente dell'amministratore del database (utilizzato dall'installazione per la creazione e la modifica del database)	Sì
--db-admin-password	Password amministratore database	Sì
--db-user-username	Nome utente del server ERA del database (utilizzato dal server ERA per la connessione al database); questo valore non deve superare 16 caratteri	Sì
--db-user-password	Password dell'utente del server ERA del database	Sì
--cert-hostname	Contiene tutti i nomi e/o gli indirizzi IP possibili del computer sul quale verrà installato il server ERA. Questo valore sarà necessario per la ricerca di una corrispondenza con il nome del server specificato nel certificato dell'agente che tenta di connettersi al server.	Sì
--server-cert-path	Percorso al certificato del peer del server (utilizzare questa opzione se è stato anche specificato il comando --salta-cert)	
--server-cert-password	Password del certificato del peer del server	
--agent-cert-password	Password del certificato del peer dell'agente	
--cert-auth-password	Password dell'autorità di certificazione	
--cert-auth-path	Percorso al file dell'autorità di certificazione del server	
--cert-auth-common-name	Nome comune dell'autorità di certificazione (utilizzare "")	
--cert-organizational-unit	-	
--cert-organization	-	

Attributo	Descrizione	Richiesto
--cert-locality	-	
--cert-state	-	
--cert-country	-	
--cert-validity	Validità del certificato in giorni o anni (specificare un argomento --unità-validità-cert)	
--cert-validity-unit	Unità per la validità del certificato, i valori possibili sono "Anni" o "Giorni" (l'impostazione predefinita è Anni)	
--ad-server	Server Active Directory	No
--ad-user-name	Nome dell'utente autorizzato a fare ricerche nella rete AD	No
--ad-user-password	Password utente Active Directory	No
--ad-cdn-include	Percorso alla struttura ad albero Active Directory per cui verrà effettuata la sincronizzazione; utilizzare le parentesi vuote "" per sincronizzare un intero albero	No

Rapporto programma di installazione

Il rapporto del programma di installazione, che rappresenta uno strumento utile per la risoluzione dei problemi, è disponibile qui:
`/var/log/eset/RemoteAdministrator/EraServerInstaller.log`

In seguito all'installazione, verificare che il servizio ERA Server sia in esecuzione:
`service eraserver status`

3.8.1.1 Prerequisiti server - Linux

Per installare il server ERA su Linux, è necessario che vengano soddisfatti i seguenti prerequisiti:

- Una licenza valida.
- Un server del database già installato e configurato con un account radice (un account utente non deve essere creato prima dell'installazione, il programma di installazione può creare l'account).
- Un driver ODBC per la connessione al server del database (MySQL/MS SQL) installato sul computer.
  `apt-get install unixodbc libmyodbc` (Distribuzioni Debian, Ubuntu)
  `yum install mysql-connector-odbc` (Distribuzioni CentOS, Red-Hat, Fedora)

NOTA: utilizzare il pacchetto **unixODBC_23** (non il pacchetto unixODBC predefinito) per consentire al server ERA di connettersi al database MySQL senza problemi. Ciò è particolarmente utile nel caso di SUSE Linux.

- File di installazione del server impostato come eseguibile.
  `chmod +x Server-Linux-i686.sh`
- La versione minima supportata di openSSL è **openssl-1.0.1e-30**
- È richiesto il pacchetto **xvfb** per una stampa corretta del report (Genera report) sui sistemi Linux Server privi di interfaccia grafica.
  `apt-get install xvfb` (Distribuzioni Debian, Ubuntu)
  `yum install xorg-x11-server-Xvfb` (Distribuzioni CentOS, Red-Hat, Fedora)
- È richiesto il pacchetto **cifs-utils** per una distribuzione corretta dell'agente su un sistema operativo Windows.
  `apt-get install cifs-utils` (Distribuzioni Debian, Ubuntu)
  `yum install cifs-utils` (Distribuzioni CentOS, Red-Hat, Fedora)
- Le **librerie Qt4 WebKit**: utilizzate per la stampa dei report in formato PDF e PS (è necessaria la versione 4.8, non la versione 5). Tutte le altre dipendenze **Qt4** verranno installate automaticamente.
  `apt-get install libqtwebkit4` (Distribuzioni Ubuntu)

NOTA: nel caso di CentOS, potrebbe non essere presente alcun pacchetto negli archivi ufficiali. È possibile installarlo da un archivio di terze parti (ad esempio, archivi EPEL) o compilarlo in modo autonomo su una macchina di destinazione.

- **Kinit + klist** utilizzato per l'autenticazione Kerberos durante l'attività di sincronizzazione AD e l'accesso con un utente del dominio. È inoltre richiesta una corretta configurazione di Kerberos (*/etc/krb5.conf*).
  `apt-get install krb5-user` (Distribuzioni Debian, Ubuntu).
  `yum install krb5-workstation` (Distribuzioni CentOS, Red-Hat, Fedora)

- **Wbinfo + ntlm_auth** utilizzato per l'autenticazione con gli account di dominio + autenticazione NTLM con server SMTP (invio di e-mail)
  `apt-get install winbind` ((Distribuzioni Debian, Ubuntu)
  `yum install samba-winbind-clients` (Distribuzioni CentOS, Red-Hat, Fedora)

- **Ldapsearch** utilizzato nell'attività di sincronizzazione AD.
  `apt-get install ldap-utils` ((Distribuzioni Debian, Ubuntu)
  `yum install openldap-clients` (Distribuzioni CentOS, Red-Hat, Fedora)

- **Snmptrap** utilizzato per inviare i trap SNMP. Facoltativo se si prevede di non utilizzare questa funzionalità. Anche l'SNMP richiede una configurazione.
  `apt-get install snmp` (Distribuzioni Ubuntu)
  `yum install net-snmp-utils` (Distribuzioni CentOS, Red-Hat, Fedora)

- Il **pacchetto SELinux devel** utilizzato durante l'installazione del prodotto per la creazione dei moduli del criterio SELinux. Questa opzione è richiesta esclusivamente sui sistemi su cui è attivo SELinux (CentOS, Fedora, RHEL).
  `apt-get install selinux-policy-dev` (Distribuzioni Debian, Ubuntu).
  `yum install policycoreutils-devel` (Distribuzioni CentOS, Red-Hat, Fedora)

NOTA: il server ERA memorizza enormi quantità di blob di dati nel database. Di conseguenza, è necessario configurare MySQL per accettare pacchetti di grandi dimensioni che garantiscano un corretto funzionamento di ERA. Per ulteriori informazioni sulle modalità di configurazione di questa funzione, consultare le Domande frequenti.

3.8.2 Installazione agente - Linux

La connessione al server ERA viene risolta utilizzando i parametri --hostname e --port (la porta non viene utilizzata quando viene fornito un record SRV). I possibili formati di connessione sono i seguenti:

- **Nome host** e **porta**
- **Indirizzo IPv4** e **porta**
- **Indirizzo IPv6** e **porta**
- Record di servizio (record SRV): per configurare il record delle risorse DNS in Linux, è necessario che il computer si trovi in un dominio con un server DNS funzionante. Consultare il capitolo Record di risorse DNS.

Il record SRV deve iniziare con il prefisso "_NOME._tcp" dove "NOME" rappresenta una denominazione personalizzata, ad esempio "era".

Di seguito viene riportato uno script di installazione di esempio. I parametri dello script sono descritti nella sezione successiva.

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/admin/Desktop/agent.pfx --cert-auth-path=/h
--cert-password=N3lluI4#2aCC --hostname=10.1.179.36 --port=2222
```

`--skip-license` farà in modo che il programma di installazione non chieda all'utente la conferma della licenza
`--cert-path` è il percorso che conduce al file del certificato dell'agente
`--cert-auth-path` è il percorso che conduce al file dell'autorità di certificazione del server
`--cert-password` deve corrispondere alla password del certificato dell'agente
`--hostname` è una connessione al server (o proxy) in uno dei seguenti formati (nome host, IPv4, IPv6 o record SRV)
`--port` è una porta di ascolto aperta sul server o sul proxy (il valore predefinito per entrambi è 2222)

Parametri facoltativi:
`--product-guid` prodotto GUID (se non definito, verrà generato)
`--cert-content` Contenuto codificato in Base64 del certificato della chiave pubblica codificata PKCS12 più chiave privata utilizzata per la configurazione di canali di comunicazione protetti con il server e gli agenti. Utilizzare solo una tra le opzioni `--cert-path` e `--cert-content`.
`--cert-auth-content` Contenuto codificato in Base64 del certificato della chiave privata dell'autorità di certificazione codificata in DER utilizzato per la verifica dei peer remoti (proxy o server). Utilizzare solo una tra le opzioni
`--cert-auth-path` e `--cert-auth-content`.
`--webconsole-hostname` nome host utilizzato dalla console Web per effettuare la connessione al server (se il campo viene lasciato vuoto, il valore verrà copiato dal campo "nome host")
`--webconsole-port` porta utilizzata dalla console Web per effettuare la connessione al server (impostazione predefinita: "2223")
`--webconsole-user` nome utente utilizzato dalla console Web per effettuare la connessione al server (impostazione predefinita: "Amministratore")
`--webconsole-password` password utilizzata dalla console Web per effettuare la connessione al server

Connessione e certificati

- È necessario fornire la **Connessione al server ERA**: `--hostname`, `--port` (la porta non è necessaria se è stato fornito il record di servizio; impostazione predefinita: "2222")
- Fornire queste informazioni di connessione per l'**Installazione assistita dal server**: --webconsole-port, --webconsole-user, --webconsole-password
- Fornire le informazioni del certificato per l'**Installazione off-line**: `--cert-path`, `--cert-password`

Parametri relativi al tipo di password

I parametri relativi al tipo di password possono essere forniti come variabili di ambiente, file, letture da stdin o come testo normale, vale a dire:
`--password=env:SECRET_PASSWORD` dove SECRET_PASSWORD è la variabile di ambiente con password
`--password=file:/opt/secret` dove la prima riga del file regolare/opt/segreto contiene la password
`--password=stdin` comunica al programma di installazione di leggere la password dall'input standard
`--password="pass:PASSWORD"` equivale a `--password="PASSWORD"` ed è obbligatorio se la password effettiva è `"stdin"` o la stringa inizia con `"env:"`, `"file:"` o `"pass:"`

Rapporto programma di installazione

Il rapporto del programma di installazione, che rappresenta uno strumento utile per la risoluzione dei problemi, è disponibile qui:
`/var/log/eset/RemoteAdministrator/EraAgentInstaller.log`

Per verificare la correttezza dell'installazione, controllare che il servizio sia attivo eseguendo il seguente comando:
`sudo service eraagent status`

3.8.2.1 Prerequisiti dell'agente - Linux

Per installare il componente agente ERA su Linux, è necessario che vengano soddisfatti i seguenti prerequisiti:

- È necessario che siano installati il server ERA ed ERA Web Console
- È necessario che sia presente un certificato per l'agente
- È necessario che sia presente un file della chiave pubblica dell'autorità di certificazione del server
- Il computer server deve essere accessibile dalla rete
- Il file di installazione dell'agente deve essere impostato come file eseguibile (a tale scopo, eseguire chmod +x sul file).
- La versione minima supportata di openssl è **openssl-1.0.1e-30**

3.8.3 Installazione di ERA Web Console - Linux

Prima di installare il componente ERA Web Console, assicurarsi che vengano soddisfatti tutti i prerequisiti:

1. Eseguire i seguenti comandi per copiare il file era.war nella cartella selezionata:
   `sudo cp era.war /var/lib/tomcat7/webapps/`
   In alternativa, è possibile estrarre i contenuti di era.war in `/var/lib/tomcat7/webapps/era/`
2. Eseguire il seguente comando per riavviare il servizio Tomcat e utilizzare il file .war, ad esempio:
   `sudo service tomcat7 restart`
3. Aprire il seguente collegamento nel browser in uso su localhost (dovrebbe comparire una schermata di accesso):
   http://localhost:8080/era

NOTA: in caso di installazione della console Web mediante il programma di installazione, l'indirizzo predefinito è:

https://localhost/era/

3.8.3.1 Prerequisiti di ERA Web Console - Linux

Per installare il componente ERA Web Console su Linux, è necessario che vengano soddisfatti i seguenti prerequisiti:

- Java: utilizzare sempre l'ultima versione di Java rilasciata ufficialmente (ERA Web Console richiede come requisito minimo Java versione 7, ma si consiglia vivamente di utilizzare l'ultima versione).
  `apt-get install openjdk-7-jdk` (Distribuzioni Debian, Ubuntu)
  `yum install java-1.8.0-openjdk` (Distribuzioni Red-Hat, Fedora)
- Apache Tomcat (versione 6 e successive)
  `sudo apt-get install tomcat7`
  `yum install tomcat7`
- File della console Web (*era.war*) salvato sul disco rigido locale.

3.8.4 Installazione proxy - Linux

1. Assicurarsi che vengano soddisfatti tutti i prerequisiti.
2. Eseguire uno script di installazione per installare il server del proxy. Di seguito viene fornito un esempio di script di installazione.

Impostazioni connessione

È necessario specificare una destinazione con un:

- Nome host
- Indirizzo IPv4
- Indirizzo IPv6
- Record di risorse DNS: il computer Linux deve trovarsi nel dominio. Consultare il capitolo Record di risorse DNS.

È necessario specificare la porta: utilizzare la porta 2222 sia per il server sia per il proxy.

Esempio di installazione
(Le nuove righe vengono separate da "\" per la copia dell'intero comando sul terminale)

```
./Proxy-Linux-x86_64-1.0.407.0.sh --db-hostname=10.1.179.28 --db-dbname=era_6_db_proxy \
--db-admin-username=sa --db-admin-password=admin.1 --db-user-username=tester \
--db-user-password=Admin.1 --db-port=1433 --db-type="MS SQL Server" \
--db-driver=SQL --skip-license --hostname=10.1.179.30 --port=2222 \
--cert-path=/home/adminko/Desktop/proxy.pfx --cert-auth-path=/home/adminko/Desktop/CA-server.der \
--cert-password=root --server-root-password=jjf#jDjr
```

È possibile modificare i seguenti attributi:

`--db-hostname` è un nome host o un indirizzo IP del server del DB
`--db-dbname` è un nome del database da utilizzare
`--db-admin-username` è un nome dell'amministratore del DB
`--db-admin-password` è una password dell'amministratore del DB
`--db-user-username` è un utente tramite il quale verrà effettuato l'accesso al DB
`--db-user-password` è la password dell'utente
`--db-port` è la porta del DB (1433 per MSSQL, 3306 per MySQL)
`--db-type` è la definizione del tipo di DB utilizzato (possibili valori: "MySQL Server" e "MS SQL Server")
`--db-driver` deve essere impostato lo stesso nome definito per MSSQL in */etc/odbcinst.ini*
`--skip-license` non chiederà all'utente la conferma della licenza
`--hostname` è un nome host o un indirizzo IP del server
`--port` è la porta del server (impostazione predefinita: 2222) o la porta del proxy (impostazione predefinita: 1236)
`--proxy-port` Porta che verrà utilizzata dal proxy (valore predefinito: "2222")
`--cert-path` è un percorso locale al file del certificato del proxy
`--cert-auth-path` è un percorso locale al file dell'AC del server
`--db-port` questa impostazione è importante ed è necessario specificarla in caso di utilizzo di MySQL. Se non viene specificata, verrà utilizzata la porta predefinita di MySQL (3306).
`-product-guid` prodotto GUID (se non definito, verrà generato)
`--cert-content` Contenuto codificato in Base64 del certificato della chiave pubblica codificata PKCS12 più chiave privata utilizzata per la configurazione di canali di comunicazione protetti con il server e gli agenti.
Utilizzare solo una tra le opzioni `--cert-path` e `--cert-content`.
`--cert-password` deve corrispondere alla password del certificato dell'agente
`--cert-auth-content` Contenuto codificato in Base64 del certificato della chiave privata dell'autorità di certificazione codificata in DER utilizzato per la verifica dei peer remoti (proxy o server). Utilizzare solo una tra le opzioni
`--cert-auth-path` e `--cert-auth-content`.
Il database `--keep-database` non verrà rimosso durante la disinstallazione

Per verificare che l'installazione sia stata eseguita correttamente, utilizzare il seguente comando che consentirà di controllare l'effettiva esecuzione del servizio:

```
sudo service eraproxy status
```

3.8.4.1 Prerequisiti proxy - Linux

Per installare il componente proxy su Linux, è necessario che vengano soddisfatti i seguenti prerequisiti:

- Il **Server ERA** ed **ERA Web Console** sono installati (su un computer server).
- Un driver ODBC per la connessione al server del database (MySQL/MS SQL) installato sul computer.
- Un server del database già installato e configurato.
- Il **Certificato del proxy** è stato creato e scaricato sull'unità locale.
- È stata preparata l'**Autorità di certificazione** sull'unità locale.
- Una licenza valida.
- Per poter supportare tutte le funzioni del programma, l'agente deve essere installato su un computer locale.
- La versione minima supportata di openssl è **openssl-1.0.1e-30**

3.8.5 Installazione e prerequisiti di RD Sensor - Linux

Per installare il componente RD Sensor su Linux, seguire la procedura sottostante:

1. Verificare che vengano soddisfatti i seguenti prerequisiti:
   - È possibile eseguire ricerche nella rete (le porte sono aperte, il firewall non blocca le comunicazioni in entrata, ecc.).
   - È possibile raggiungere il computer server.
   - Per poter supportare tutte le funzioni del programma, l'Agente ERA deve essere installato sul computer locale.
   - Il terminale è aperto.
2. Utilizzare il seguente comando per eseguire il file di installazione come sudo:

```
sudo ./RDSensor-Linux-x86_64-1.0.223.0.sh
```

3. Per verificare la correttezza dell'installazione, controllare che il servizio sia attivo eseguendo il seguente comando:

```
sudo service rdsensor status
```

4. Rogue Detection Sensor verrà installato sul computer in uso.
5. Il file di rapporto di Rogue Detection Sensor è disponibile in: *var/log/eset/RemoteAdministrator/RogueDetectionSensor/trace.log*

3.8.6 Installazione di Connettore dispositivi mobili - Linux

Connettore dispositivi mobili può essere installato su un server differente da quello in cui è in esecuzione il server ERA. Ad esempio, se si desidera rendere Connettore dispositivi mobili accessibile da Internet in modo da poter gestire i dispositivi mobili dell'utente in qualsiasi momento.

L'installazione del componente Server ERA su Linux viene eseguita attraverso un comando nel terminale. Assicurarsi che vengano soddisfatti tutti i prerequisiti. È possibile preparare uno script di installazione ed eseguirlo utilizzando il comando *sudo*.

Molti parametri di installazione sono facoltativi, ma alcuni di essi sono obbligatori.

Per eseguire l'installazione, è richiesto il certificato del peer ERA. Per ottenerlo, è possibile procedere in due modi:

- **Installazione assistita dal server**: sarà necessario fornire le credenziali amministratore di ERA Web Console (i certificati richiesti saranno scaricati automaticamente).
- **Installazione off-line**: sarà necessario fornire un certificato del peer (il Certificato dell'agenteesportato da ESET Remote Administrator). In alternativa, è possibile utilizzare il proprio certificato personalizzato.

È necessario fornire i seguenti parametri del comando di installazione:

Certificato HTTPS:

```
--https-cert-path=
--https-cert-password=
```

Certificato del peer:
Per un'**Installazione assistita dal server** includere almeno:

```
--webconsole-password=
```

Per un'**Installazione off-line** includere:

```
--cert-path=
```

`--cert-password=` (la password non è necessaria per il certificato dell'agente predefinito creato durante l'installazione iniziale del server ERA)

Connessione al server ERA (nome o indirizzo IP):

```
--hostname=
```

Per un database MySQL includere:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Per un database MSSQL includere:

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Se esiste già un database MySQL/MSSQL, includere:

```
--db-use-existing-db=
```

oppure

```
--db-drop-existing-db=
```

Esempio

(Le nuove righe vengono separate da "\" per la copia dell'intero comando sul terminale)

```
sudo ./MDMCore-Linux-x86_64-0.0.0.0.sh \
--https-cert-path="./httpscert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--db-use-existing-db \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

Per un elenco completo dei parametri disponibili (stampa messaggio della guida), usare:

```
--help
```

Rapporto programma di installazione

Il rapporto del programma di installazione, che rappresenta uno strumento utile per la risoluzione dei problemi, è disponibile qui:

```
/var/log/eset//mdminstaller.log
```

Al termine dell'installazione, verificare la corretta esecuzione di Connettore dispositivi mobili aprendo https://*your-mdm-hostname*:*enrollment-port* (ad esempio *https://eramdm:9980*) nel browser Web. Se l'installazione è stata eseguita correttamente, verrà visualizzato il seguente messaggio:

MDM Server up and running!

È anche possibile utilizzare questo URL per verificare la disponibilità del server Connettore dispositivi mobili da Internet (se configurato in tal modo) visitandolo da un dispositivo mobile. Se non si riesce a visualizzare la pagina, controllare il firewall e la configurazione dell'infrastruttura di rete.

3.8.6.1 Prerequisiti di Connettore dispositivi mobili - Linux

Per installare il Connettore dispositivi mobili su Linux, è necessario che vengano soddisfatti i seguenti prerequisiti:

- Un server del database già installato e configurato con un account radice (un account utente non deve essere creato prima dell'installazione, il programma di installazione può creare l'account).
- Un driver ODBC per la connessione al server del database (MySQL/MS SQL) installato sul computer.
  `apt-get install unixodbc libmyodbc` (Distribuzioni Debian, Ubuntu)
  `yum install mysql-connector-odbc` (Distribuzioni CentOS, Red-Hat, Fedora)

NOTA: utilizzare il pacchetto **unixODBC_23** (non il pacchetto unixODBC predefinito) per consentire al server ERA di connettersi al database MySQL senza problemi. Ciò è particolarmente utile nel caso di SUSE Linux.

- File di installazione del server impostato come eseguibile.
  `chmod +x MDMCore-Linux-i686.sh`
- In seguito all'installazione, verificare che il servizio MDMCore sia in esecuzione.
  `service mdmcore status`
- La versione minima supportata di openSSL è **openssl-1.0.1e-30**

NOTA: il server ERA memorizza enormi quantità di blob di dati nel database. Di conseguenza, è necessario configurare MySQL per accettare pacchetti di grandi dimensioni che garantiscano un corretto funzionamento di ERA. Per ulteriori informazioni sulle modalità di configurazione di questa funzione, consultare le Domande frequenti.

IMPORTANTE: sarà necessario un **certificato SSL** in formato `PFX` per comunicazioni sicure su HTTPS. Si consiglia l'utilizzo di un certificato fornito da un'autorità di certificazione (AC). L'uso dei certificati autofirmati è sconsigliato poiché non tutti i dispositivi mobili consentono agli utenti di accettare certificati autofirmati. Questo problema non si verifica con i certificati firmati da un'autorità di certificazione poiché sono attendibili e non richiedono l'accettazione da parte dell'utente.

IMPORTANTE: per l'Installazione off-line sarà necessario fornire anche un certificato del peer (il **Certificato dell'agente**esportato da ESET Remote Administrator). In alternativa, è possibile utilizzare il proprio certificato personalizzato con ERA.

3.8.7 Installazione del proxy Apache HTTP - Linux

Per installare il componente proxy Apache HTTP su Windows, attenersi alla procedura che segue:

1. Installare il server Apache HTTP (versione minima: 2.4.10)
2. Caricare i seguenti moduli: access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile, authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
3. Aggiungere la configurazione della cache:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Se la directory */var/cache/apache2/mod_cache_disk* non esiste, crearla e assegnare i privilegi Apache (r,w,x)
5. Aggiungere la configurazione del proxy:

```
ProxyRequests On
ProxyVia On

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Attivare la configurazione aggiunta (se la configurazione si trova in configurazione principale, saltare questo passaggio)
7. Se necessario, modificare l'ascolto sulla porta desiderata (la porta 3128 è l'impostazione predefinita)
8. Autenticazione facoltativa di base:
   - Aggiungere la configurazione dell'autenticazione alla directory del proxy:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

   - Creare un file della password utilizzando `htpasswd.exe -c`
   - Creare manualmente un file denominato group.file con `usergroup:username`
9. Riavviare il server

Server Ubuntu 14.10:

1. `sudo apt-get install apache2`
2. `sudo a2enmod access_compat auth_basic authn_core authn_file authz_core authz_groupfile \ authz_host proxy proxy_http proxy_connect cache cache_disk`
3. `sudo vim /etc/apache2/conf-available/caching.conf`
   - copiare/incollare la configurazione della cache:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Questo passaggio non è obbligatorio. Tuttavia, se la directory della cache non esiste, è necessario eseguire i seguenti comandi:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. `sudo vim /etc/apache2/conf-available/proxy.conf`
   - copiare/incollare la configurazione del proxy:

```
ProxyRequests On
ProxyVia On

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. `sudo a2enconf caching.conf proxy.conf`
7. `sudo vim /etc/apache2/ports.conf`
   - sostituire `Listen 80` con `Listen 3128`
8. Autenticazione facoltativa di base:
   - `sudo vim /etc/apache2/conf-available/proxy.conf`

     copiare/incollare la configurazione dell'autenticazione prima di `</Proxy>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

```
sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user
sudo vim /etc/apache2/group.file
insert: usergroup:user
```

```
9.sudo service apache2 restart
```

Impostazioni generali:

Consentire l'inoltro solo per le comunicazioni ESET:

1. Sostituire i valori che seguono nella configurazione del proxy:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

con:

```
<Proxy *>
Deny from all
</Proxy>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\. \
[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\. \
[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2. \
mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net|edf-pcs.cloudapp.net|edf-pcs2.clouda
edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?(87.106.247.14|209.157.66.250|209.157.66.253| \
212.227.134.125|212.227.134.126|212.227.134.128|212.227.134.130|212.227.134.131|212.227.134.132| \
212.227.134.133|212.227.134.158)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
```

Concatenamento del proxy (tutto il traffico):

Aggiungere i valori che seguono alla configurazione del proxy (la password funziona solo su un proxy figlio):

```
ProxyRemote * http://10.1.172.26:3128
```

Squid3:

1. Installare Squid3
2. Aggiungere `cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000` alla configurazione sotto a `cache_dir` (5000 è la dimensione della cache in MB)
3. Creare una cartella della cache con squid: `squid3 -z` (interrompere il servizio squid3 se in esecuzione)
4. Aggiungere Consenti accesso per i client desiderati
5. Riavviare squid3

Server Ubuntu 14.10:

```
1.sudo apt-get install squid3
```

```
2.sudo vim /etc/squid3/squid.conf
```

sostituire `#cache_dir ufs /var/spool/squid3 100 16 256` con `cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000`

```
3.sudo service squid3 stop

    sudo squid3 -z

4.sudo vim /etc/squid3/squid.conf
```

Aggiungere `http_access allow all` prima di `http_access deny all` per consentire a tutti di accedere al proxy

```
5.sudo service squid3 restart
```

3.8.8 Come disinstallare o reinstallare un componente - Linux

Se si desidera eseguire una reinstallazione o un aggiornamento a una versione più recente, eseguire nuovamente lo script di installazione.

Per disinstallare un componente (in questo caso il server ERA), eseguire il programma di installazione con il parametro **--uninstall**, come illustrato di seguito:

```
sudo ./Server-Linux-i686.sh --uninstall --keep-database
```

Se si desidera disinstallare un altro componente, utilizzare il nome del pacchetto appropriato nel comando. Ad esempio l'a

```
sudo ./Agent-Linux-x86_64.sh --uninstall
```

Attenzione: durante la disinstallazione, i file di configurazione e del database verranno rimossi. Per preservare file del database, creare un dump SQL del database oppure utilizzare il parametro `--keep-database`.

In seguito alla disinstallazione, controllare

- che il servizio `eraserverService.sh` sia stato eliminato.
- che la cartella `/etc/opt/eset/RemoteAdministrator/Server/` sia stata eliminata.

Si consiglia di creare una copia di backup del dump del database prima di eseguire la disinstallazione qualora si desideri ripristinare i dati.

3.9 Record servizio DNS

Per configurare un Record di risorse DNS:

1. Sul server DNS (server DNS sul controller di dominio), accedere a **Pannello di controllo** > **Strumenti di amministrazione**.
2. Selezionare il valore DNS.
3. Nel DNS Manager, selezionare *_tcp* dalla struttura ad albero e creare un nuovo record **Posizione del servizio (SRV**).
4. Inserire il nome del servizio nel campo **Servizio** in base alle regole DNS standard, digitare un simbolo di sottolineatura (**_**) davanti al nome del servizio (utilizzare il proprio nome di servizio, ad esempio **_era**).
5. Inserire il protocollo tcp nel campo **Protocollo** nel seguente formato: *_tcp*.
6. Inserire la porta 2222 nel campo **Numero porta**.
7. Inserire il Nome di dominio completo (FQDN) del server ERA nel campo **Host che offre il servizio**.
8. Salvare il record facendo clic su [**OK**], quindi su [**Fine**]. A questo punto, il record verrà visualizzato nell'elenco.

Per verificare il record DNS:

1. Accedere a un computer qualsiasi del dominio e aprire un prompt dei comandi (*cmd.exe*).
2. Digitare *nslookup* nel prompt dei comandi e premere **Invio**.
3. Digitare *set querytype=srv* e premere **Invio**.
4. Digitare *_era._tcp.domain.name* e premere **Invio**. La posizione del servizio verrà visualizzata correttamente.

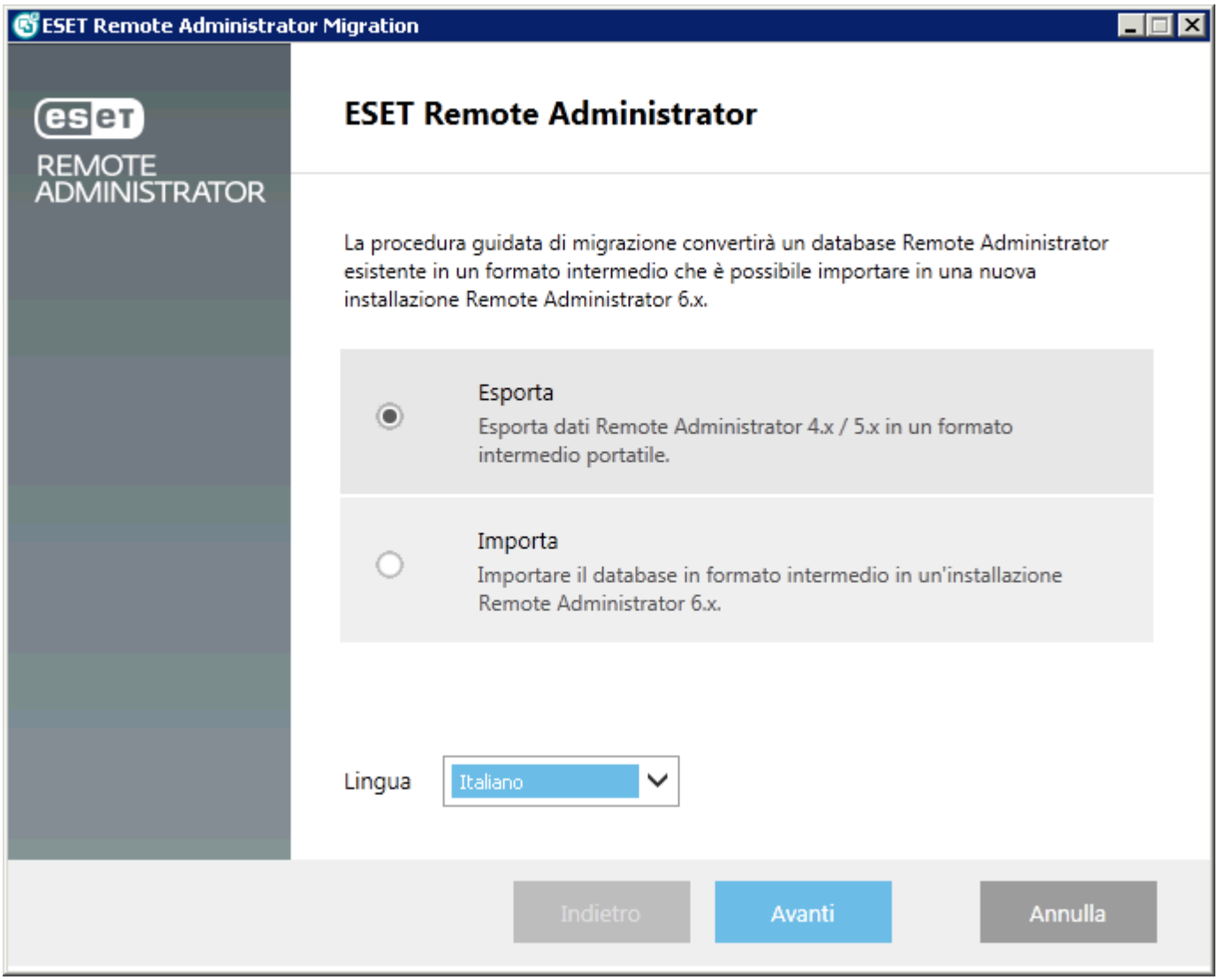
NOTA: questa procedura è identica per Windows e Linux.

NOTA: non dimenticare di modificare il valore "Host che offre il servizio:" sull'FQDN del nuovo server durante l'installazione del server ESET Remote Administrator su un'altra macchina.

3.10 Strumento di migrazione

La procedura di migrazione guidata è un'applicazione indipendente che consente una migrazione diretta dei dati di ERA 4.x/5.x in un database intermedio e permette all'utente di importarli in ERA 6.x.

Scaricare ESET Remote Administrator Migration Tool. Per scaricare lo strumento, è necessario essere in possesso del nome utente e della password ESET esistenti.

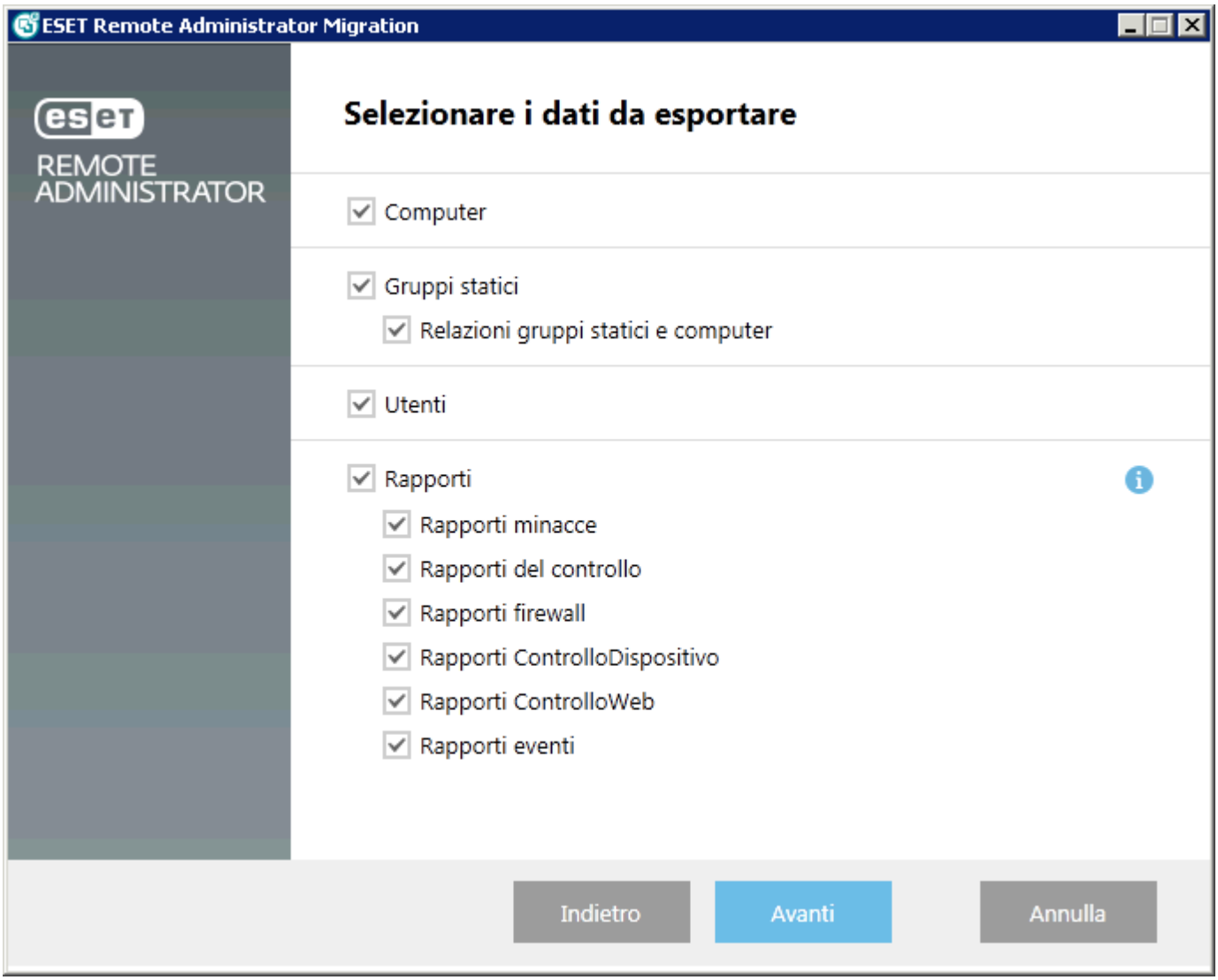

ESET Remote Administrator Migration
REMOTE ADMINISTRATOR
ESET Remote Administrator
La procedura guidata di migrazione convertirà un database Remote Administrator esistente in un formato intermedio che è possibile importare in una nuova installazione Remote Administrator 6.x.
Esporta
Esporta dati Remote Administrator 4.x / 5.x in un formato intermedio portatile.
Importa
Importare il database in formato intermedio in un'installazione Remote Administrator 6.x.
Lingua
Italiano
Indietro
Avanti
Annulla

NOTA: per risolvere il problema del file `MSVCP100.dll` oppure `MSVCR100.dll` mancante, installare la versione più recente di Microsoft Visual C++ 2010 Redistributable Package. È possibile utilizzare il seguente collegamento Microsoft Visual C++ 2010 Redistributable Package (x86).

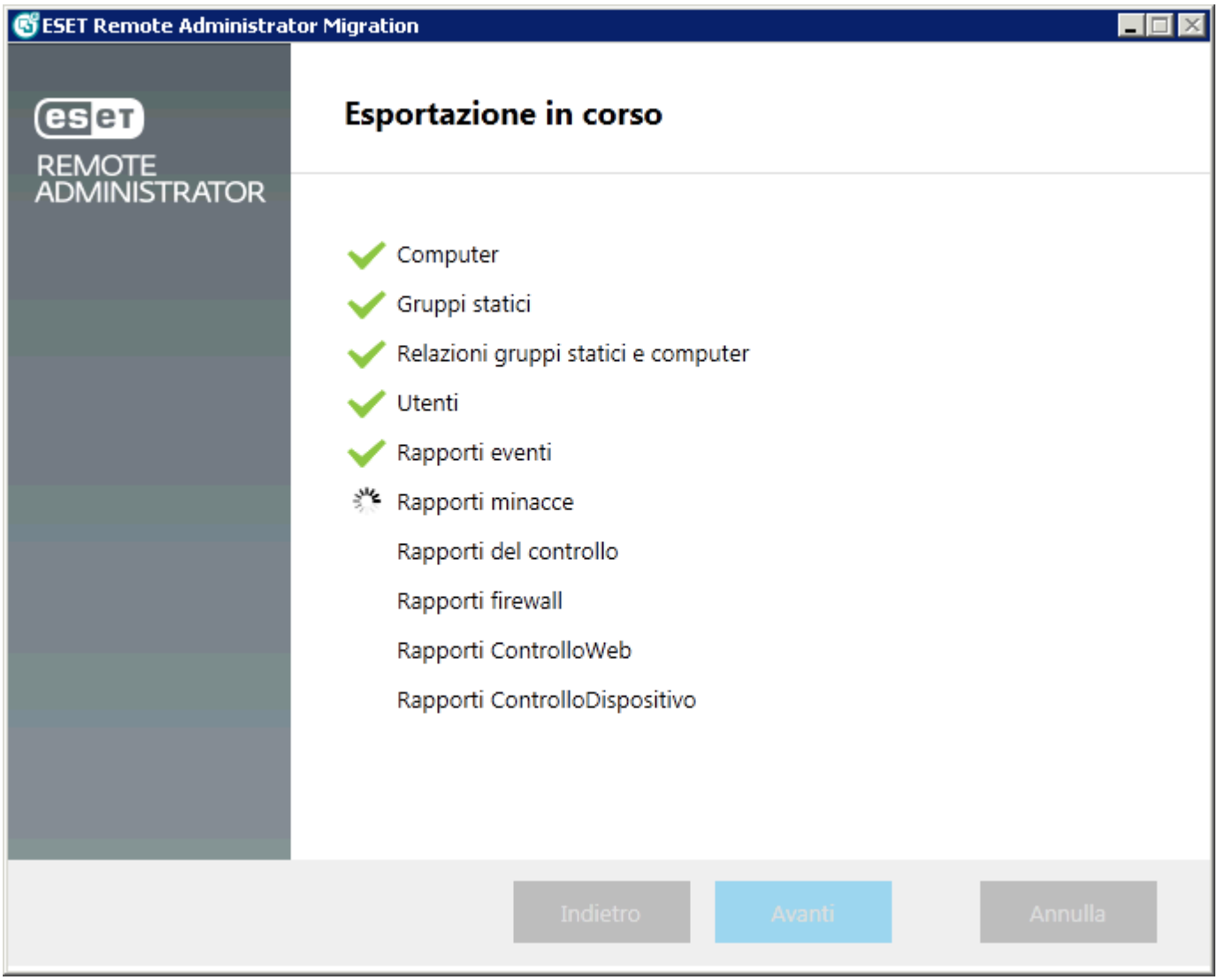
3.10.1 Scenario di migrazione 1

Questo scenario contempla una migrazione a ERA 6.x in esecuzione su un computer differente da ERA 4.x/5.x.

1. La prima operazione da eseguire nella procedura di migrazione consiste nel verificare che ERA 6.x sia installato e in esecuzione su un altro computer.
2. Avviare lo strumento di migrazione di ESET Remote Administrator sulla macchina ERA 4.x / 5.x e selezionare **Esporta** per salvare i dati dalla versione ERA precedente nel file di database intermedio.
3. La procedura di migrazione guidata consente di trasferire solo dati specifici. Selezionare i dati che si desiderano trasferire e fare clic su Avanti.



A causa del nuovo design e della funzionalità dei Gruppi dinamici in ERA 6.x, non è possibile trasferire i gruppi parametrici, le attività e i criteri da versioni precedenti. Dopo aver selezionato una cartella dove salvare il database temporaneo, verrà visualizzato lo stato dell'archivio del database ERA 4.x/5.x.



Tutti i dati sono esportati su un **database intermedio**.

4. Al termine dell'esportazione dei dati è possibile scegliere tra due opzioni:
   - Un'opzione disponibile è **Fine** per terminare l'esportazione, **Copiare** il file del database temporaneo su un server sul quale è in esecuzione ESET Remote Administrator 6.x e importare i dati tramite lo strumento di migrazione ERA su tale server.
   - In alternativa, è possibile fare clic sul pulsante **Importa ora** e importare i dati direttamente in ESET Remote Administrator 6.x tramite la rete. Specificare la connessione e i dati di accesso del nuovo server ERA.

NOTA: i Gruppi statici sincronizzati da Active Directory sono ignorati e non saranno esportati.

- Se le impostazioni del server non consentono di importare dati specifici, lo strumento di migrazione di ESET Remote Administrator consente di modificare le impostazioni di componenti specifici di ERA 6x.
- Ciascuno dei componenti viene quindi importato. Per ciascun componente è disponibile un **rapporto di importazione (migrazione)**. Al termine dell'importazione, verranno visualizzati i risultati della procedura.
- Nel caso in cui si dovesse eseguire la migrazione di utenti, le relative password vengono reimpostate e sostituite con password generate casualmente. Tali password possono essere esportate in formato `.csv`.
- La procedura guidata dello strumento di migrazione genera inoltre uno script che può essere utilizzato per preconfigurare gli agenti ERA sulle macchine client. Lo script è un file `.bat` eseguibile di piccole dimensioni che può essere distribuito sui computer client.
- È consigliabile rivedere le impostazioni e i dati per i quali è stata eseguita la migrazione per verificare che l'importazione sia stata eseguita correttamente. È quindi possibile utilizzare questo script per distribuire l'agente ERA su un gruppo ristretto di computer per verificare se si connettono correttamente al server.

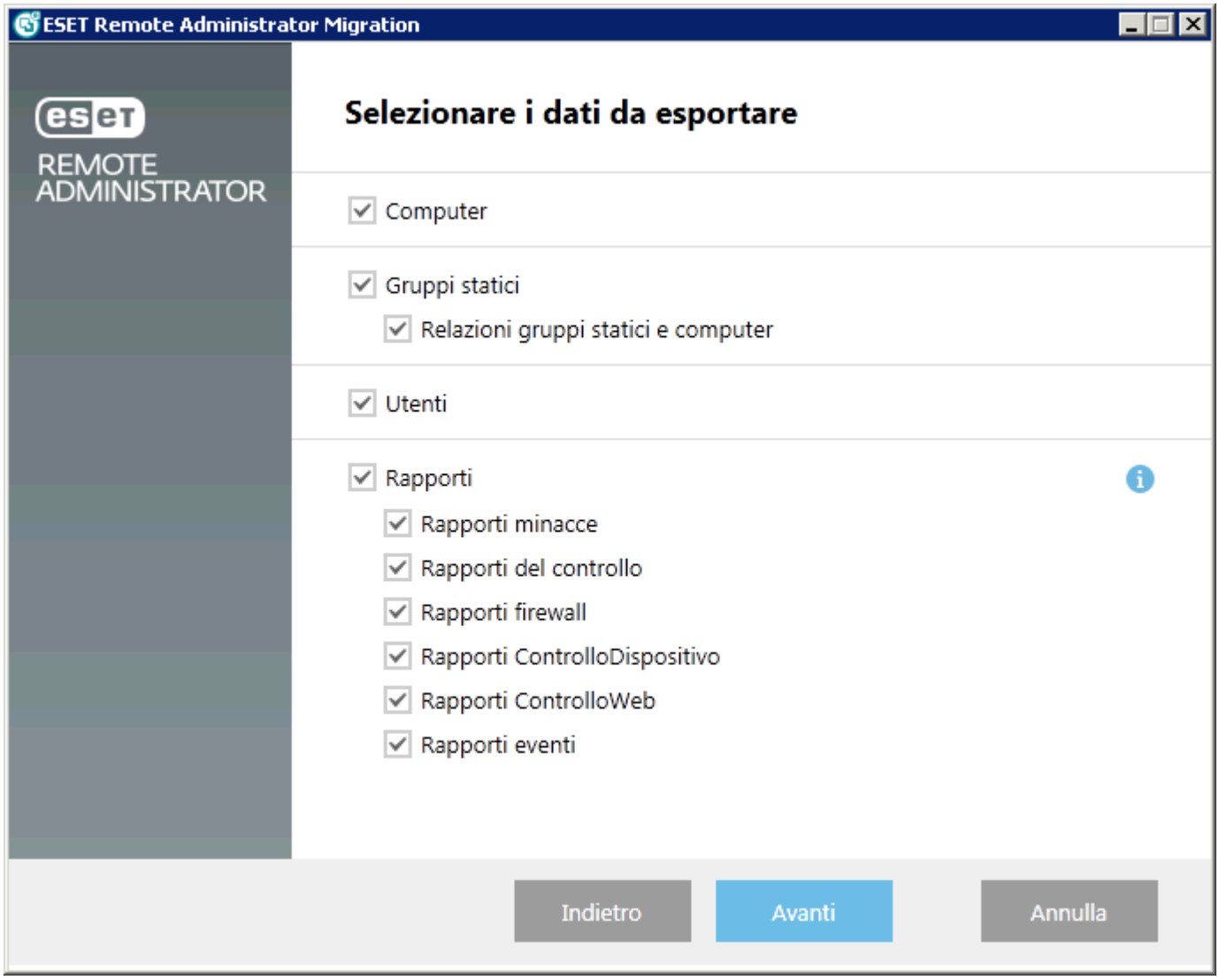
- Dopo aver connesso correttamente il gruppo di test, è possibile distribuire l'agente ai restanti computer, manualmente o tramite l'attività di sincronizzazione AD.

NOTA: nel caso in cui uno qualsiasi dei restanti passaggi non dovesse riuscire, è necessario annullare le modifiche apportate a ERA 6.x, configurare i computer per la connessione a ERA 4.x/5.x, recuperare i dati di backup da ERA 4.x/5.x e contattare il supporto tecnico ESET.

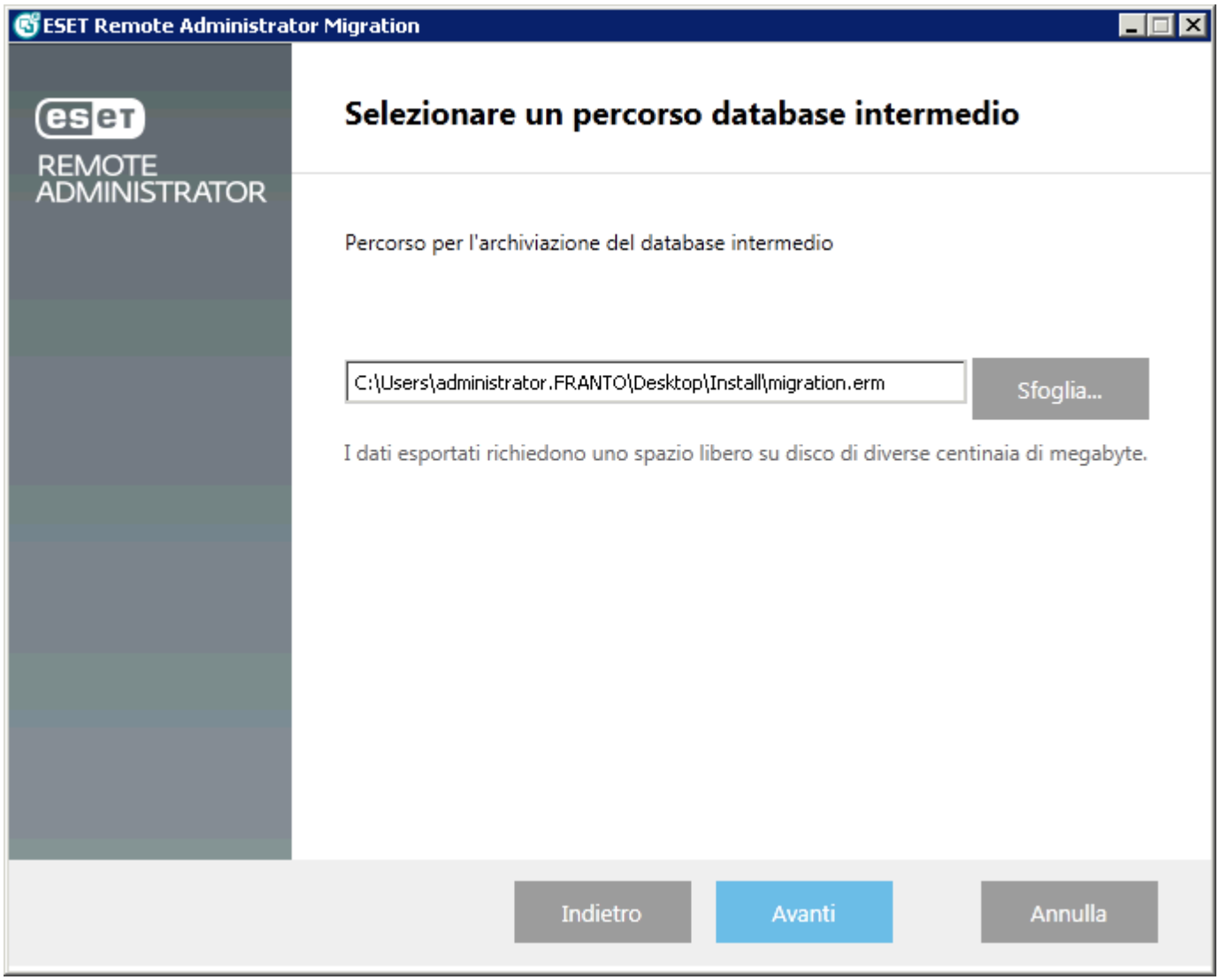
3.10.2 Scenario di migrazione 2

Questo scenario contempla una migrazione a ESET Remote Administrator 6.x in esecuzione sullo stesso computer su cui è eseguito ERA 4.x/5.x. Prima di eseguire la migrazione dei dati, è necessario aver eseguito il backup di tutti i dati (tramite lo strumento di manutenzione ESET) e aver interrotto i servizi ERA nel sistema operativo.

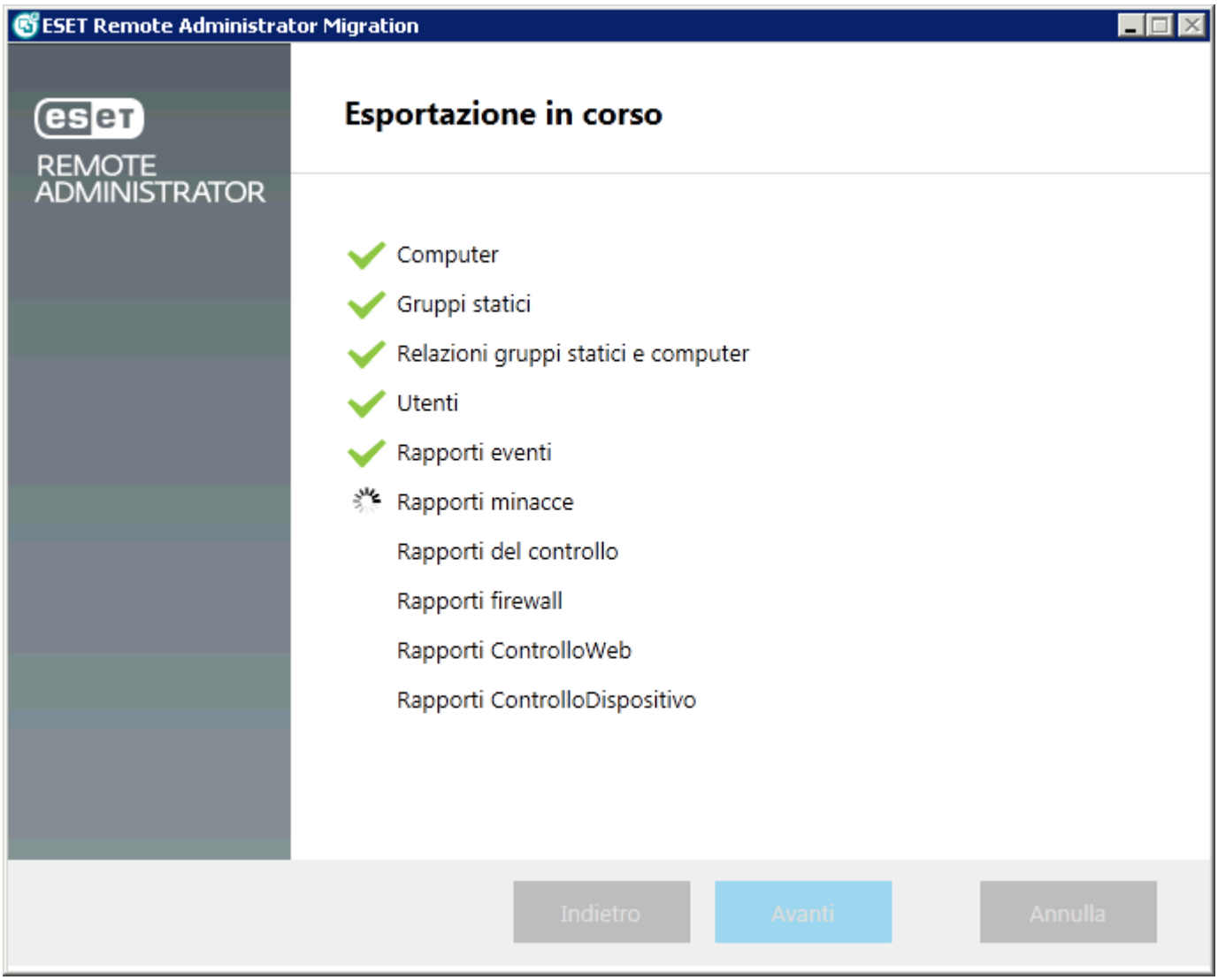
1. Dopo aver avviato lo strumento di migrazione di ESET Remote Administrator sulla macchina ERA 4.x / 5.x, l'amministratore seleziona l'opzione **Esporta** per salvare i dati da ERA 4.x/5.x su un file di database intermedio. La procedura di migrazione guidata consente di trasferire solo dati specifici:



NOTA: a causa del nuovo design e della funzionalità dei Gruppi dinamici in ERA 6.x, non è possibile trasferire i gruppi parametrici, le attività e i criteri da ERA 4.x/5.x.



2. Dopo aver selezionato una cartella dove salvare il database temporaneo, la procedura guidata consentirà di visualizzare lo stato di archiviazione del database ERA 4.x/5.x.



3. Tutti i dati sono esportati su un **database intermedio**.

- Dopo aver **esportato** correttamente i dati e prima di **distribuire** ERA 6.x, è necessario aver **disinstallato** ERA 4.x/5.x.
- Quando la nuova versione ERA 6.x è stata installata, il database esportato può essere importato utilizzando lo strumento di migrazione. All'amministratore viene chiesto di selezionare il file salvato.
- Se le impostazioni del server non consentono di importare dati specifici, lo strumento di migrazione di ESET Remote Administrator consente di modificare le impostazioni di componenti specifici di ERA 6x.
- Ciascuno dei componenti viene quindi importato. Per ciascun componente è disponibile un **rapporto di importazione (migrazione)**. Al termine dell'importazione, verranno visualizzati i risultati della procedura.
- Nel caso in cui si dovesse eseguire la migrazione di utenti, le relative password vengono reimpostate e sostituite con password generate casualmente. Tali password possono essere esportate in formato `.csv`.
- La procedura guidata dello strumento di migrazione genera inoltre uno script che può essere utilizzato per preconfigurare gli agenti ERA sulle macchine client. Lo script è un file `.bat` eseguibile di piccole dimensioni che può essere distribuito sui computer client.
- È consigliabile rivedere le impostazioni e i dati per i quali è stata eseguita la migrazione per verificare che l'importazione sia stata eseguita correttamente. È quindi possibile utilizzare questo script per distribuire l'agente ERA su un gruppo ristretto di computer per verificare se si connettono correttamente al server.

- Dopo aver connesso correttamente il gruppo di test, è possibile distribuire l'agente ai restanti computer, manualmente o tramite l'attività di sincronizzazione AD.

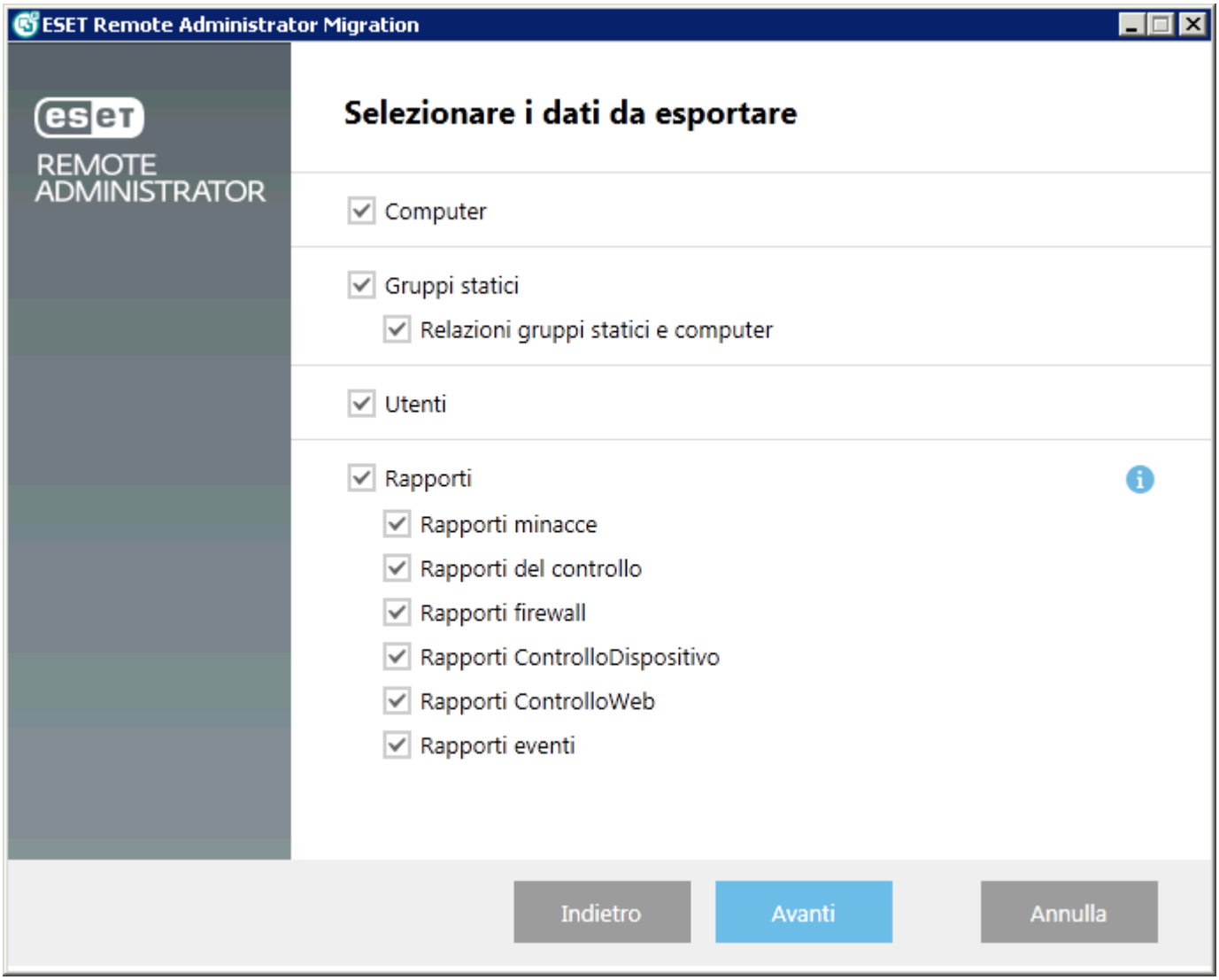
NOTA: nel caso in cui uno qualsiasi dei restanti passaggi non dovesse riuscire, è necessario annullare le modifiche apportate a ERA 6.x, configurare i computer per la connessione a ERA 4.x/5.x, recuperare i dati di backup da ERA 4.x/5.x e contattare il supporto tecnico ESET.

3.10.3 Scenario di migrazione 3

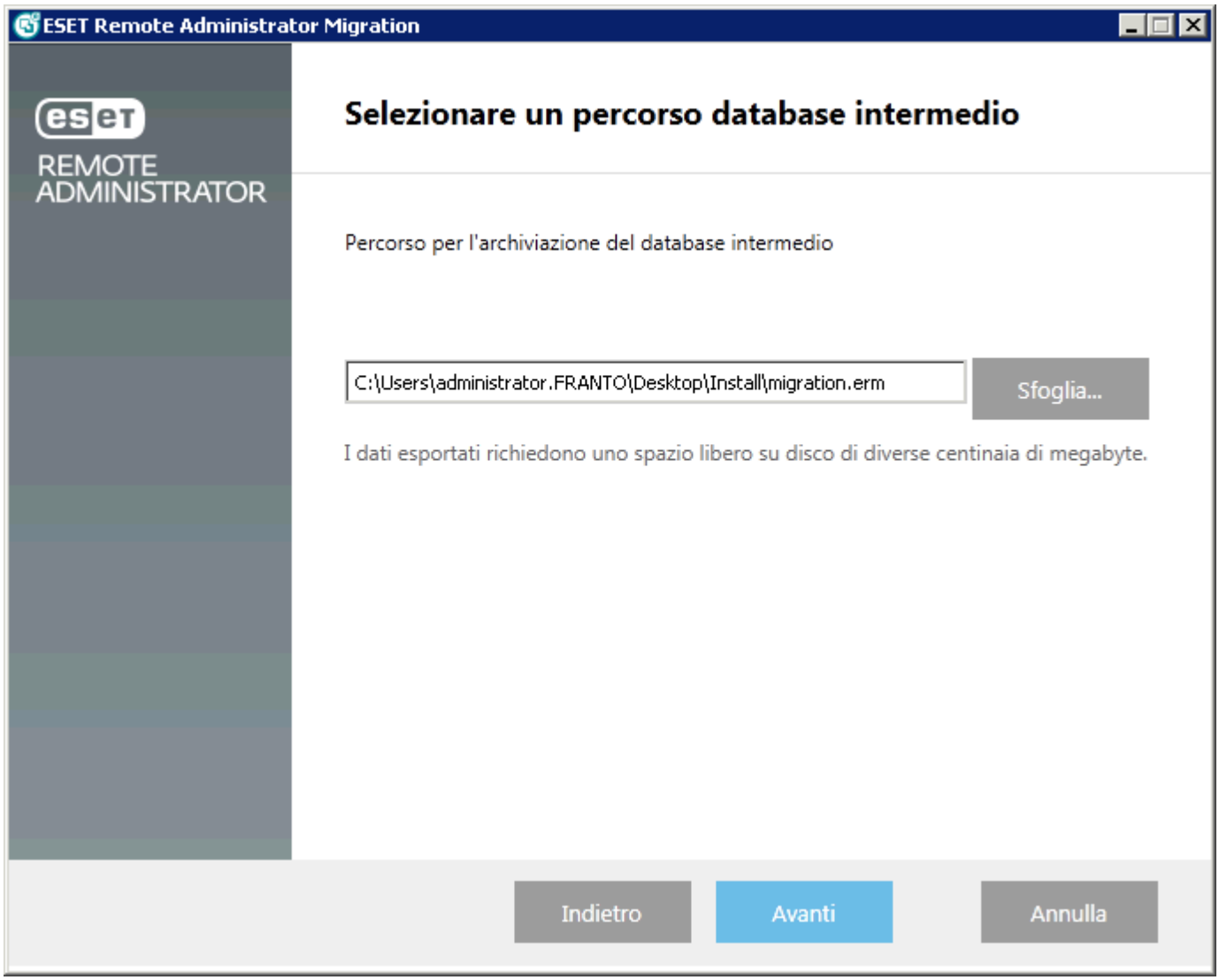
Questo scenario contempla una migrazione a ERA 6.x dove gli endpoint si connettono alla versione ERA 4.x/5.x precedente fino a quando ERA 6.x distribuisce l'agente ERA.

NOTA: questo scenario è consigliato esclusivamente agli utenti esperti. Non è consigliabile eseguire questo tipo di migrazione, a meno che non siano disponibili altre opzioni.

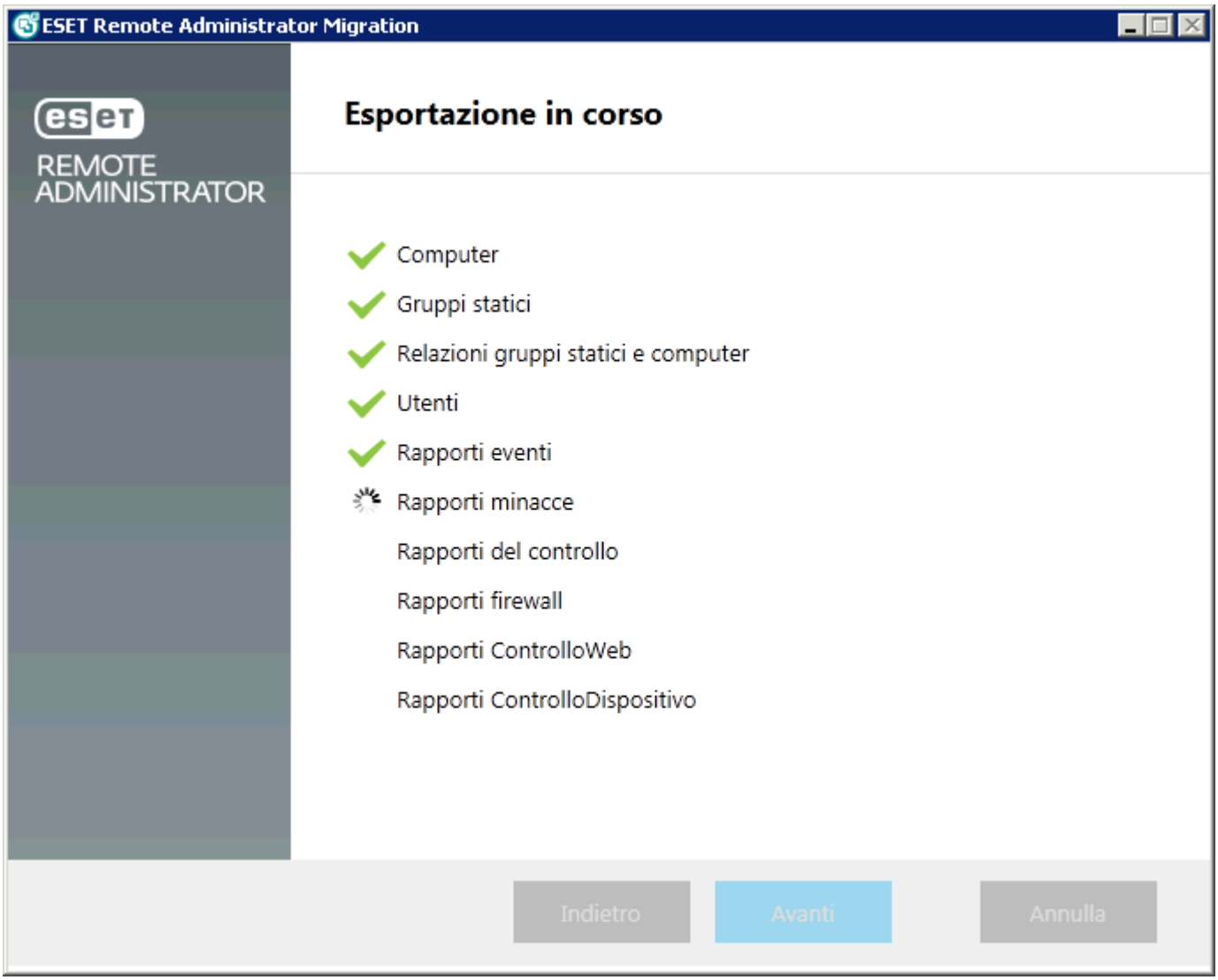
1. Dopo aver avviato lo strumento di migrazione di ESET Remote Administrator sulla macchina ERA 4.x / 5.x, l'amministratore seleziona l'opzione **Esporta** per salvare i dati da ERA 4.x/5.x su un file di database intermedio. La procedura di migrazione guidata consente di trasferire solo dati specifici:



NOTA: a causa del nuovo design e della funzionalità dei Gruppi dinamici in ERA 6.x, non è possibile trasferire i gruppi parametrici, le attività e i criteri da ERA 4.x/5.x.



2. Dopo aver selezionato una cartella dove salvare il database temporaneo, la procedura guidata consentirà di visualizzare lo stato di archiviazione del database ERA 4.x/5.x.



3. Tutti i dati sono esportati su un **database intermedio**.
4. Se ERA 6 verrà installato sullo stesso computer sul quale è installata la versione 4.x/5.x, è necessario modificare le porte della versione ERA precedente e rinominare il servizio del server (`sc config ERA_SERVER DisplayName= "ESET Remote Administrator g1"`).
5. ESET Remote Administrator 4.x/5.x deve essere nuovamente avviato in seguito all'esportazione dei dati dell'utente.
6. Installare ESET Remote Administrator 6 e importare il database intermedio tramite lo strumento di migrazione.
   - Se le impostazioni del server non consentono di importare dati specifici, lo strumento di migrazione di ESET Remote Administrator consente di modificare le impostazioni di componenti specifici di ERA 6x.
   - Ciascuno dei componenti viene quindi importato. Per ciascun componente è disponibile un **rapporto di importazione (migrazione)**. Al termine dell'importazione, verranno visualizzati i risultati della procedura.
   - Nel caso in cui si dovesse eseguire la migrazione di utenti, le relative password vengono reimpostate e sostituite con password generate casualmente. Tali password possono essere esportate in formato `.csv` .
   - La procedura guidata dello strumento di migrazione genera inoltre uno script che può essere utilizzato per preconfigurare gli agenti ERA sulle macchine client. Lo script è un file `.bat` eseguibile di piccole dimensioni che può essere distribuito sui computer client.

- È consigliabile rivedere le impostazioni e i dati per i quali è stata eseguita la migrazione per verificare che l'importazione sia stata eseguita correttamente. È quindi possibile utilizzare questo script per distribuire l'agente ERA su un gruppo ristretto di computer per verificare se si connettono correttamente al server.
- Dopo aver connesso correttamente il gruppo di test, è possibile distribuire l'agente ai restanti computer, manualmente o tramite l'attività di sincronizzazione AD.

NOTA: nel caso in cui uno qualsiasi dei restanti passaggi non dovesse riuscire, è necessario annullare le modifiche apportate a ERA 6.x, configurare i computer per la connessione a ERA 4.x/5.x, recuperare i dati di backup da ERA 4.x/5.x e contattare il supporto tecnico ESET.

A seguito di questo tipo di migrazione non ci saranno rapporti esportati tra il processo di backup del database di ERA 4.x/5.x e la distribuzione dell'agente su un computer client. Tali dati saranno tuttavia ancora presenti sulla copia precedente di ERA 4.x/5.x.

4. Primi passi

Dopo aver installato correttamente ESET Remote Administrator, è possibile passare alla fase di impostazione delle varie opzioni. I capitoli che seguono illustreranno i passi iniziali raccomandati da seguire dopo l'installazione di ESET Remote Administrator.

Innanzitutto, aprire ERA Web Console nel browser Web ed effettuare l'accesso.

Conoscere ERA Web Console

Prima di avviare la configurazione iniziale, si consiglia di acquisire dimestichezza con ERA Web Console, che rappresenta l'interfaccia che verrà utilizzata per la gestione delle soluzioni di protezione ESET.

Aggiungere computer client, server e dispositivi mobili presenti nella rete alla struttura ERA
Durante l'installazione, è possibile ricercare computer (client) nella rete. I client trovati saranno elencati nella sezione Computer in cui verrà avviato ESET Remote Administrator. Se i client non compaiono nella sezione Computer, eseguire l'attività Sincronizzazione gruppi statici per ricercare i computer e visualizzarli in gruppi.

Distribuzione di un agente
Dopo aver trovato i computer client, distribuire l'agente. L'agente fornisce la comunicazione tra ESET Remote Administrator e i client.

Installazione del prodotto ESET (include l'attivazione)
Per preservare la sicurezza dei client e della rete, installare i prodotti ESET. Questa operazione è resa possibile grazie all'attività Installazione software.

Creazione/modifica di gruppi
Si consiglia di ordinare i client in Gruppi statici o dinamici utilizzando vari criteri. Ciò consente di facilitare la gestione dei client e di avere una panoramica della rete.

Creazione di un nuovo criterio
Se si desidera forzare una specifica configurazione di un prodotto ESET in esecuzione sui computer client, l'utilizzo dei criteri si rivela estremamente utile. Queste risorse consentono all'utente di evitare di configurare manualmente il prodotto ESET di ciascun client, attraverso la forzatura della configurazione. Dopo aver creato un nuovo criterio con la configurazione personalizzata, è possibile assegnarlo a un gruppo (statico o dinamico). Il criterio viene quindi applicato a tutti i computer del gruppo.

Assegnazione di un criterio a un gruppo
Come illustrato in precedenza, per poter applicare un criterio, è necessario assegnarlo a un gruppo. Ai computer che appartengono al gruppo verrà applicato il criterio in questione. Il criterio verrà applicato tutte le volte che un agente che si connette al server ERA.

Configurazione delle notifiche e creazione dei report
Per avere un quadro più chiaro di ciò che accade sui computer client nell'ambiente di lavoro, si consiglia di utilizzare le notifiche e i report (se si desidera, ad esempio, ricevere la notifica dell'occorrenza di uno specifico evento oppure visualizzare o scaricare un report).

4.1 Aprire ERA Web Console

Esistono vari modi per aprire ERA Web Console:

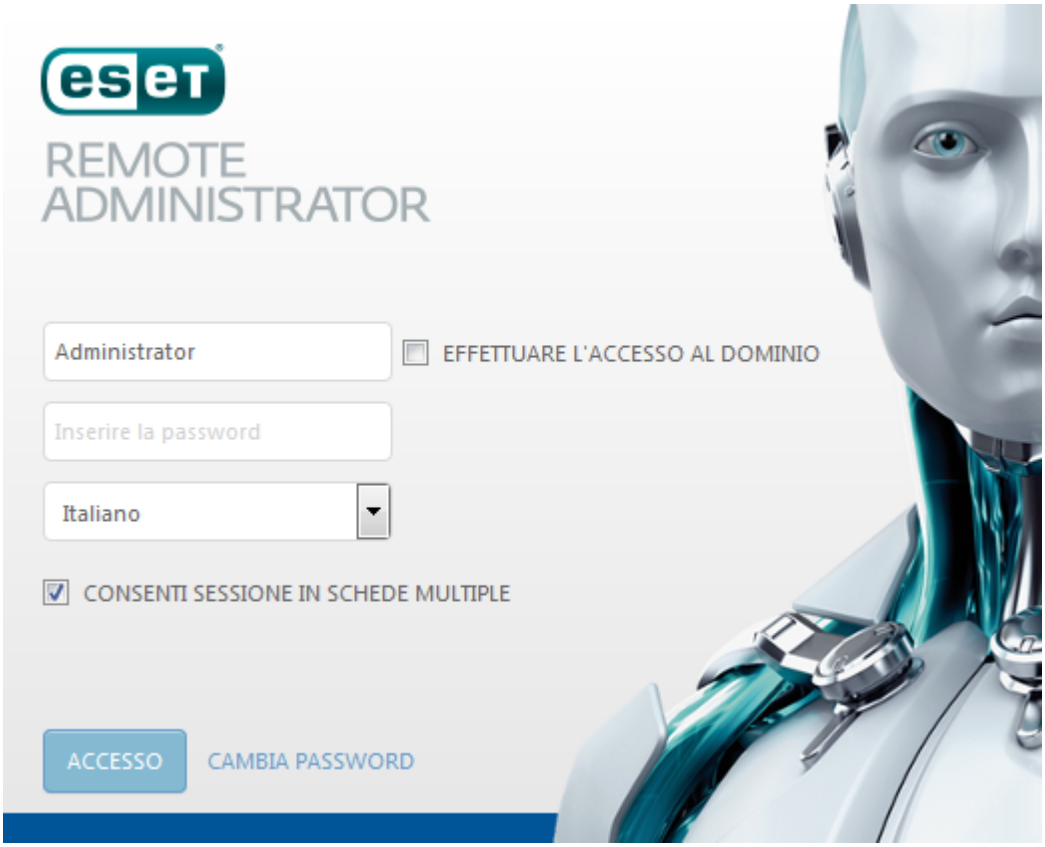
- Sul server locale (la macchina che ospita la console Web), digitare il seguente URL nel browser Web: *https://localhost/era/*

- Da qualsiasi postazione dotata di accesso a Internet, accedere al server Web e digitare l'URL nel seguente formato: *https://yourservername/era/*
  Sostituire "yourservername" con il nome effettivo o l'indirizzo IP del server Web.

- Per accedere a ERA Virtual Appliance, utilizzare il seguente URL:
  https://[IP address]:8443/
  Sostituire "[IP address]" con l'indirizzo IP di ERA VM. Nel caso in cui non si ricordi l'indirizzo IP, consultare il passaggio 9 delle istruzioni relative alla distribuzione degli accessori virtuali.
- Sul server locale (la macchina che ospita la console Web), fare clic su Avvio > **Tutti i programmi** > **ESET** > **ESET Remote Administrator** > **ESET Remote Administrator Webconsole**: si aprirà una schermata di accesso nel browser Web predefinito. Tale operazione non si applica a ERA Virtual Appliance.

NOTA: dal momento che la console Web utilizza un protocollo sicuro (HTTPS), nel browser Web potrebbe comparire un messaggio relativo a un certificato di protezione o a una connessione non attendibile (le parole esatte del messaggio dipendono dal browser in uso). Ciò dipende dal fatto che il browser desidera verificare l'identità del sito al quale si tenta di accedere. Fare clic su **Continuare con il sito Web** (Internet Explorer) o **Comprendo i rischi** , su **Aggiungi eccezione...**, quindi su **Conferma eccezione di sicurezza** (Firefox) per consentire l'accesso a ERA Web Console. Questa condizione si applica nel momento in cui si tenta di accedere all'URL di ESET Remote Administrator Web Console.

Quando il server Web (su cui viene eseguita ERA Web Console) è attivo, verrà visualizzata la seguente schermata.

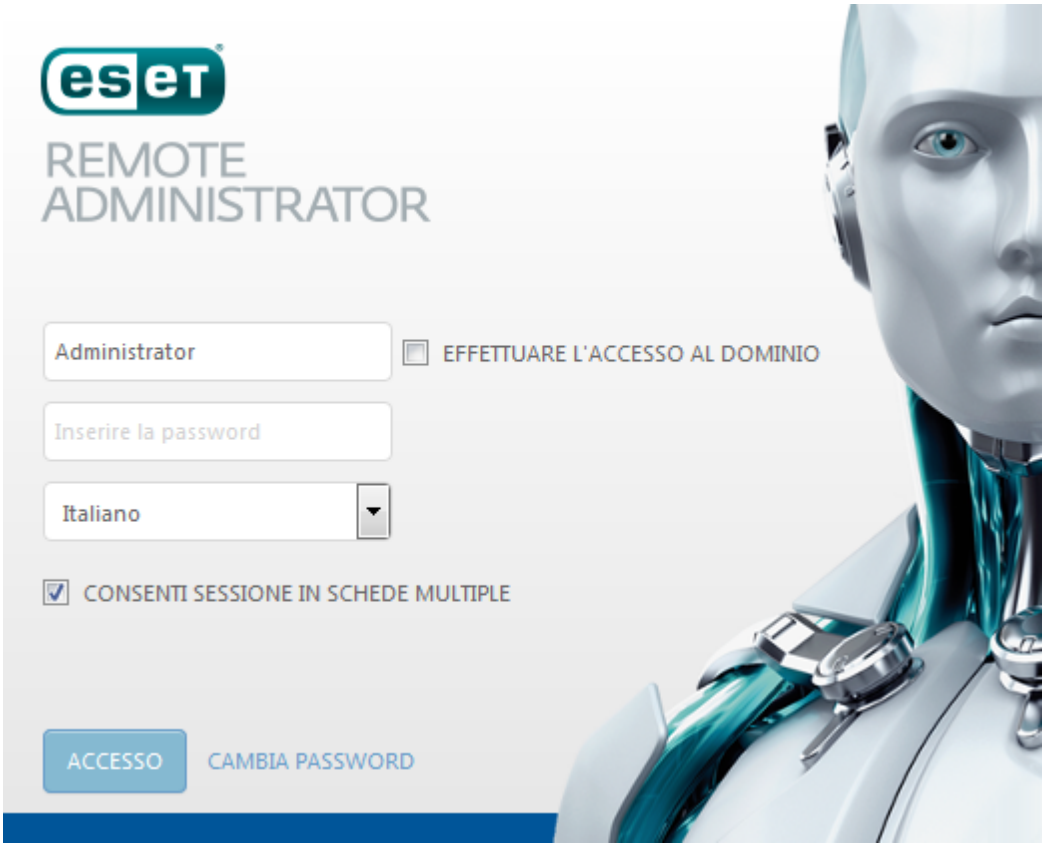


In caso di primo accesso, fornire le credenziali inserite durante il Processo di installazione. Per ulteriori informazioni su questa schermata, consultare Schermata di accesso console Web.

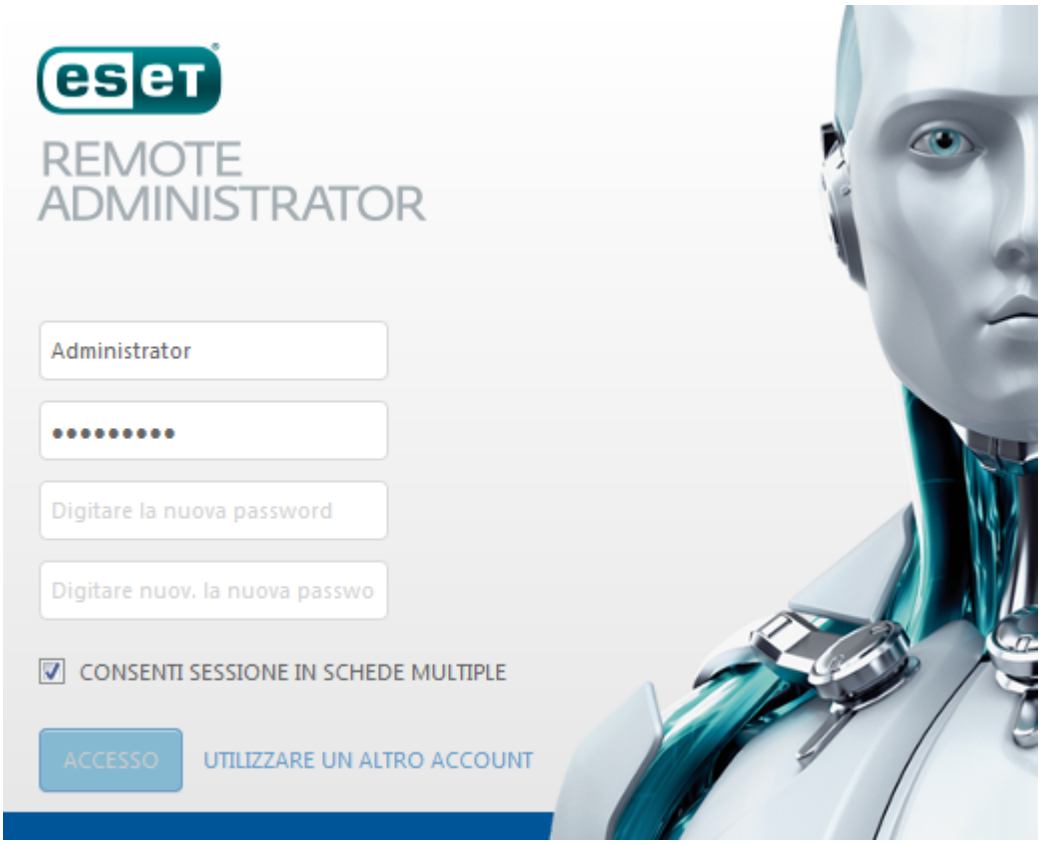
NOTA: nel raro caso in cui la schermata di accesso non venga visualizzata o rimanga bloccata sulla schermata di caricamento, riavviare il servizio *ESET Remote Administrator Server*. Quando il servizio *ESET Remote Administrator Server* è nuovamente attivo, riavviare il servizio *Apache Tomcat*. La schermata di accesso alla console Web verrà quindi caricata correttamente.

4.2 Schermata di accesso di ERA Web Console

Per accedere alla console Web, è necessario inserire le credenziali di accesso (nome utente e password). È inoltre possibile accedere come utente del dominio selezionando la casella di controllo accanto a **Effettuare l'accesso al dominio** (un utente del dominio non è correlato ad alcun gruppo del dominio mappato). È possibile selezionare la lingua da un elenco posizionato nell'angolo in alto a destra della schermata di accesso. Selezionare **Consenti sessione in schede multiple** per consentire agli utenti di aprire ERA Web Console in varie schede nel browser Web utilizzato.



Cambia password/Prova con un altro account: consente di cambiare la password o ritornare alla schermata di accesso. Un utente non in possesso di un set di autorizzazioni potrà accedere alla console Web ma non visualizzare le informazioni contenute.



Per concedere all'utente autorizzazioni di lettura/scrittura/modifica nei moduli della console Web, è necessario creare e assegnare un Set di autorizzazioni adeguato.

Gestione della sessione e misure di protezione:

- **Blocco indirizzo IP di accesso**

Dopo 10 tentativi di accesso non riusciti dallo stesso indirizzo IP, gli ulteriori tentativi da tale indirizzo sono momentaneamente bloccati per circa 10 minuti. Il blocco dell'indirizzo IP sui tentativi di accesso non influenza le sessioni esistenti.

- **Blocco indirizzo ID sessione errato**

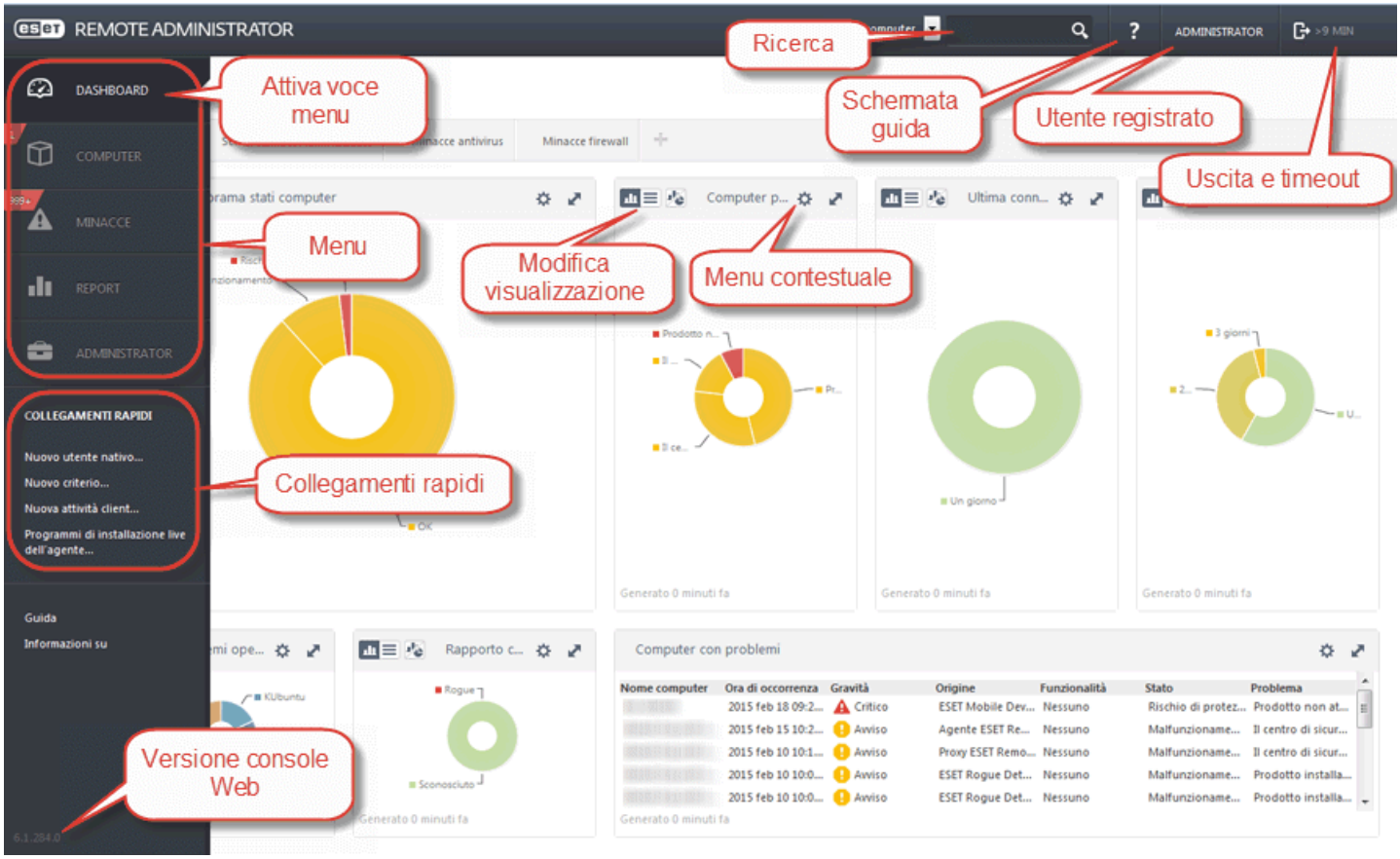
Dopo aver utilizzato 15 volte un ID sessione non valido dallo stesso indirizzo IP, tutte le ulteriori connessioni da tale indirizzo sono bloccate per circa 15 minuti. Gli ID delle sessioni scadute non vengono conteggiati. Se nel browser è presente un ID sessione scaduto, non viene considerato come un attacco. Il blocco dell'indirizzo IP per 15 minuti è attivo per tutte le azioni (comprese le richieste valide).

4.3 Conoscere ERA Web Console

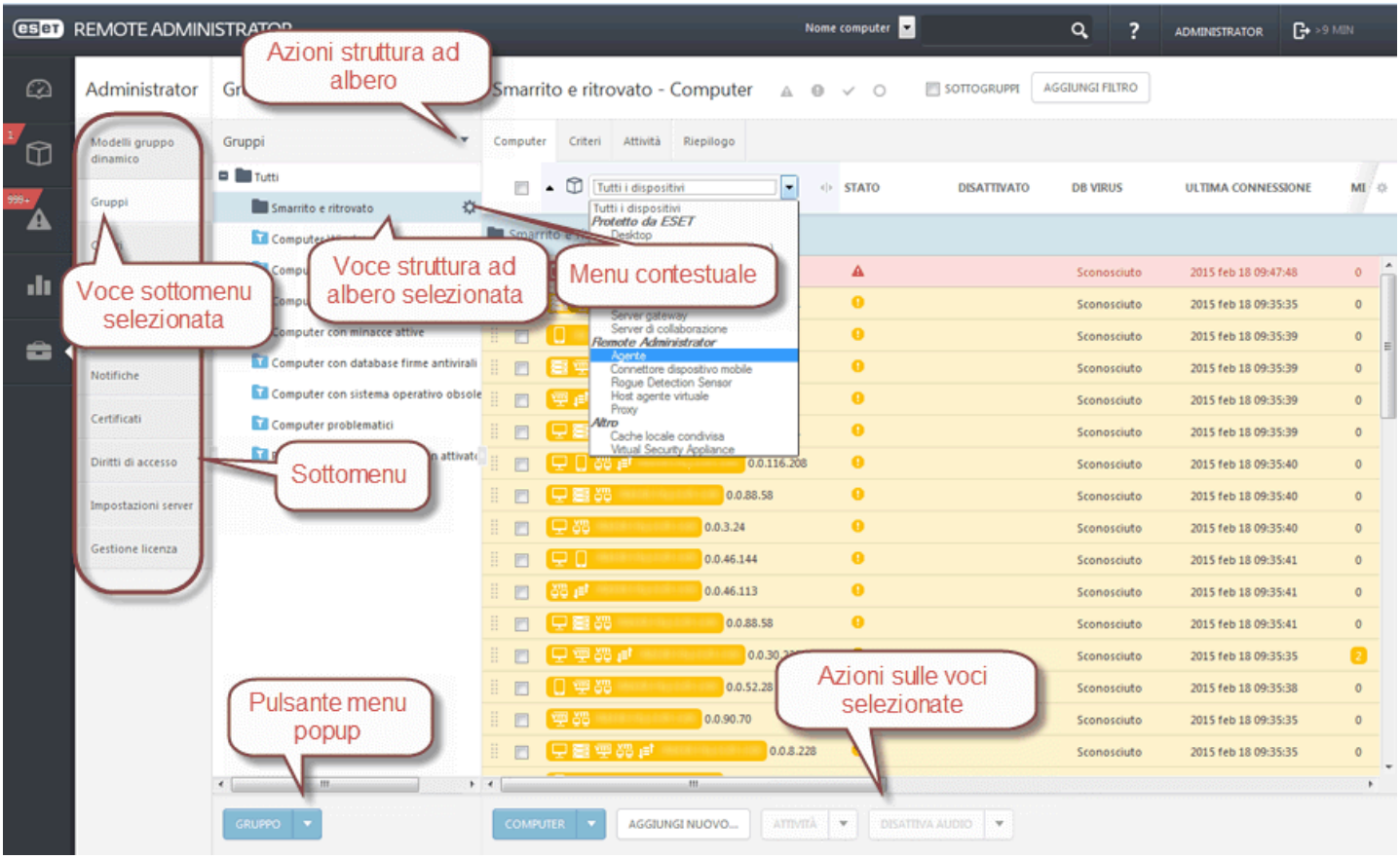
ESET Remote Administrator Web Console è la principale interfaccia di connessione a ERA Server. È possibile immaginarla come un pannello di controllo, una centrale dalla quale è possibile gestire tutte le soluzioni di protezione ESET. È un'interfaccia basata sul Web alla quale è possibile accedere tramite browser (vedere Browser Web supportati) da qualsiasi punto e dispositivo dotato di accesso a Internet.

I principi di base dell'orientamento della GUI sono:

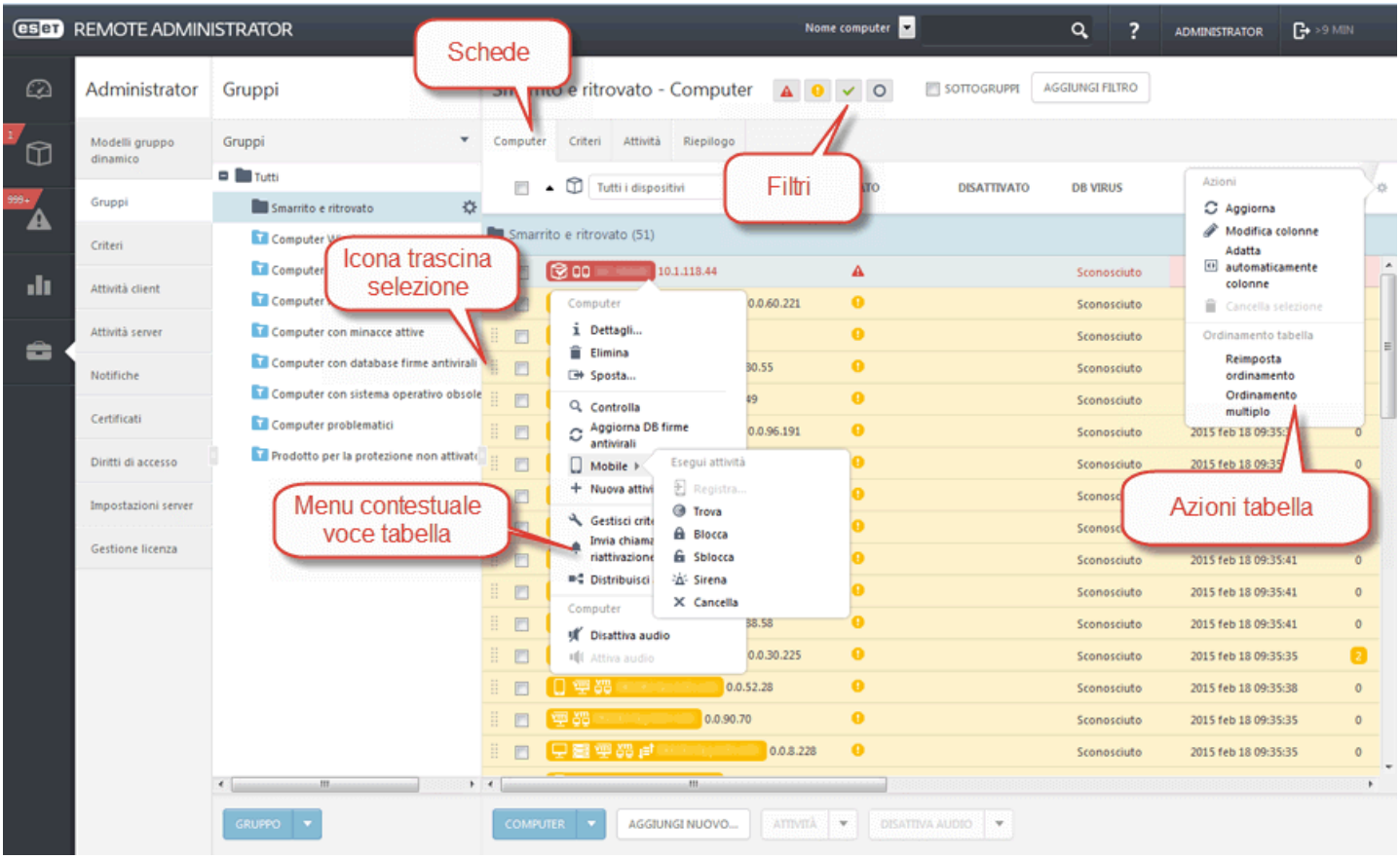
- L'utente attualmente registrato viene visualizzato sempre nell'angolo in alto a destra, in cui è disponibile un conto alla rovescia fino al timeout della sessione. In qualsiasi momento è possibile fare clic su **Esci** accanto al conto alla rovescia per disconnettersi. In caso di scadenza della sessione (a causa dell'inattività dell'utente), l'utente dovrà effettuare nuovamente l'accesso.
- Fare clic su **?** nella parte superiore di qualsiasi finestra per visualizzare la **schermata della guida** di tale schermata.
- Il **Menu** è sempre accessibile sulla sinistra, ad eccezione di quando si utilizza una procedura guidata. In qualsiasi momento, posizionare il mouse sul lato sinistro della schermata per visualizzare il menu. I menu contengono anche **Collegamenti rapidi** e l'indicazione della **versione della console Web.**
- Un'icona a forma di rotella indica sempre la presenza di un menu contestuale.



Le schermate con struttura ad albero contengono comandi specifici. Le strutture ad albero si trovano sulla sinistra e le relative azioni sono elencate in basso. Fare clic su un elemento della struttura ad albero per visualizzare le relative opzioni.

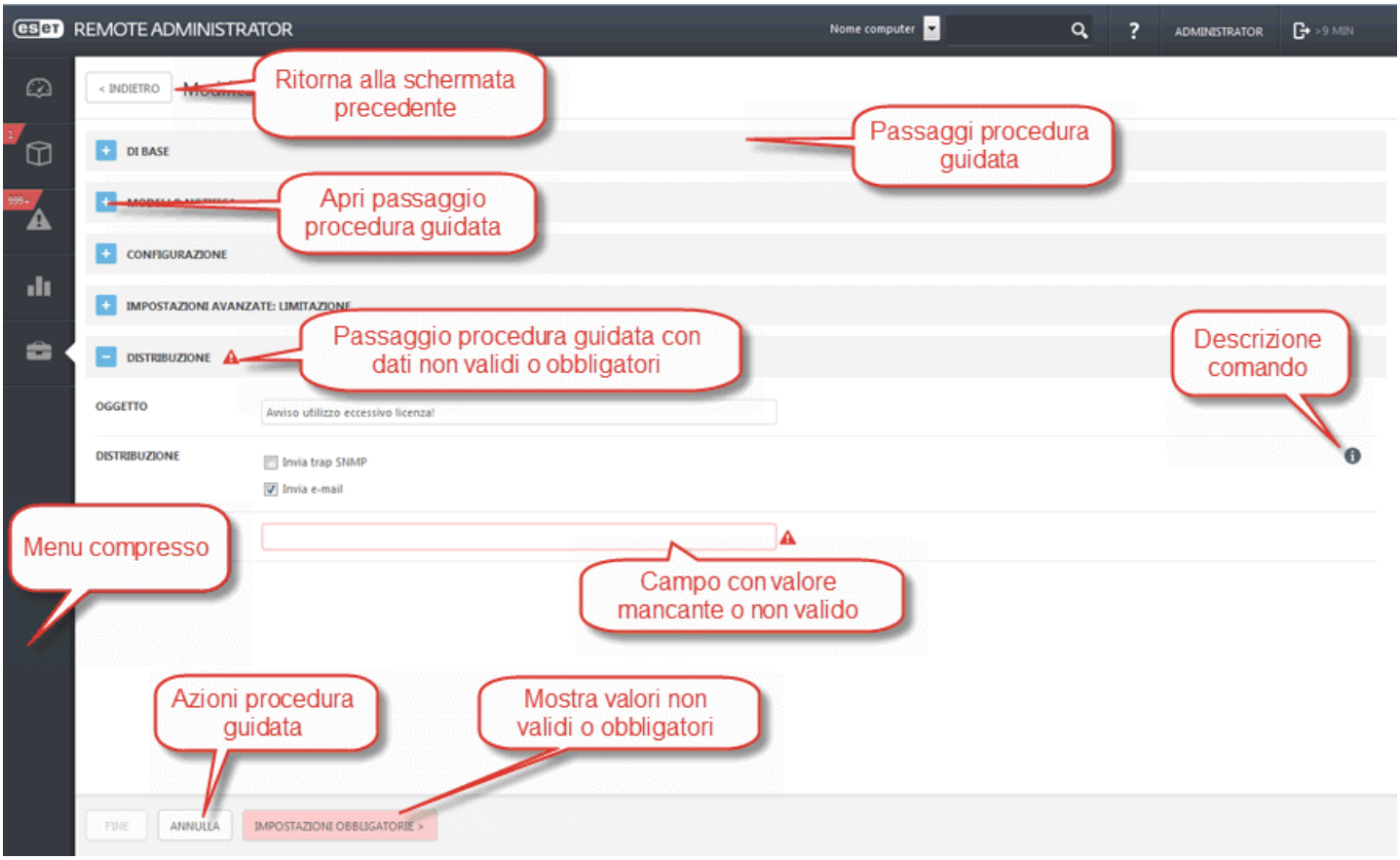


Le tabelle consentono di gestire le unità dalle relative righe prese singolarmente o in gruppo (in caso di selezione di più di una riga). Fare clic su una riga per visualizzare le opzioni per le unità di tale riga. I dati contenuti nelle tabelle possono essere filtrati e ordinati.



Gli oggetti presenti in ERA possono essere modificati mediante l'utilizzo delle procedure guidate. Tutte le procedure guidate condividono alcuni comportamenti comuni:

- I passaggi sono orientati in modo verticale dall'alto verso il basso.
- L'utente può ritornare in qualsiasi momento su ciascun passaggio.
- Quando si sposta il cursore su un nuovo campo, i dati di inserimento non validi vengono contrassegnati. È contrassegnata anche la fase della procedura guidata contenente dati di inserimento non validi.
- L'utente può controllare in qualsiasi momento i dati non validi facendo clic su **Impostazioni obbligatorie**.
- Il pulsante Fine non è disponibile finché tutti i dati non saranno corretti.



4.4 Distribuzione

Dopo aver installato correttamente ESET Remote Administrator, è necessario effettuare la distribuzione dell'**Agente ERA**e di **ESET Endpoint Protection (EES, EEA...)** sui computer presenti nella rete. La distribuzione viene effettuata in base ai seguenti passaggi:

1. Aggiungere computer client alla struttura dei gruppi di ESET Remote Administrator.
2. Distribuzione dell'agente ERA
3. Distribuzione di ESET Endpoint Protection

Dopo aver eseguito la distribuzione dell'agente ERA, è possibile installare altri prodotti di protezione ESET da remoto sui computer client. I passaggi relativi all'installazione da remoto sono descritti nel capitolo Installazione prodotto.

4.4.1 Aggiungere un computer client alla struttura ERA

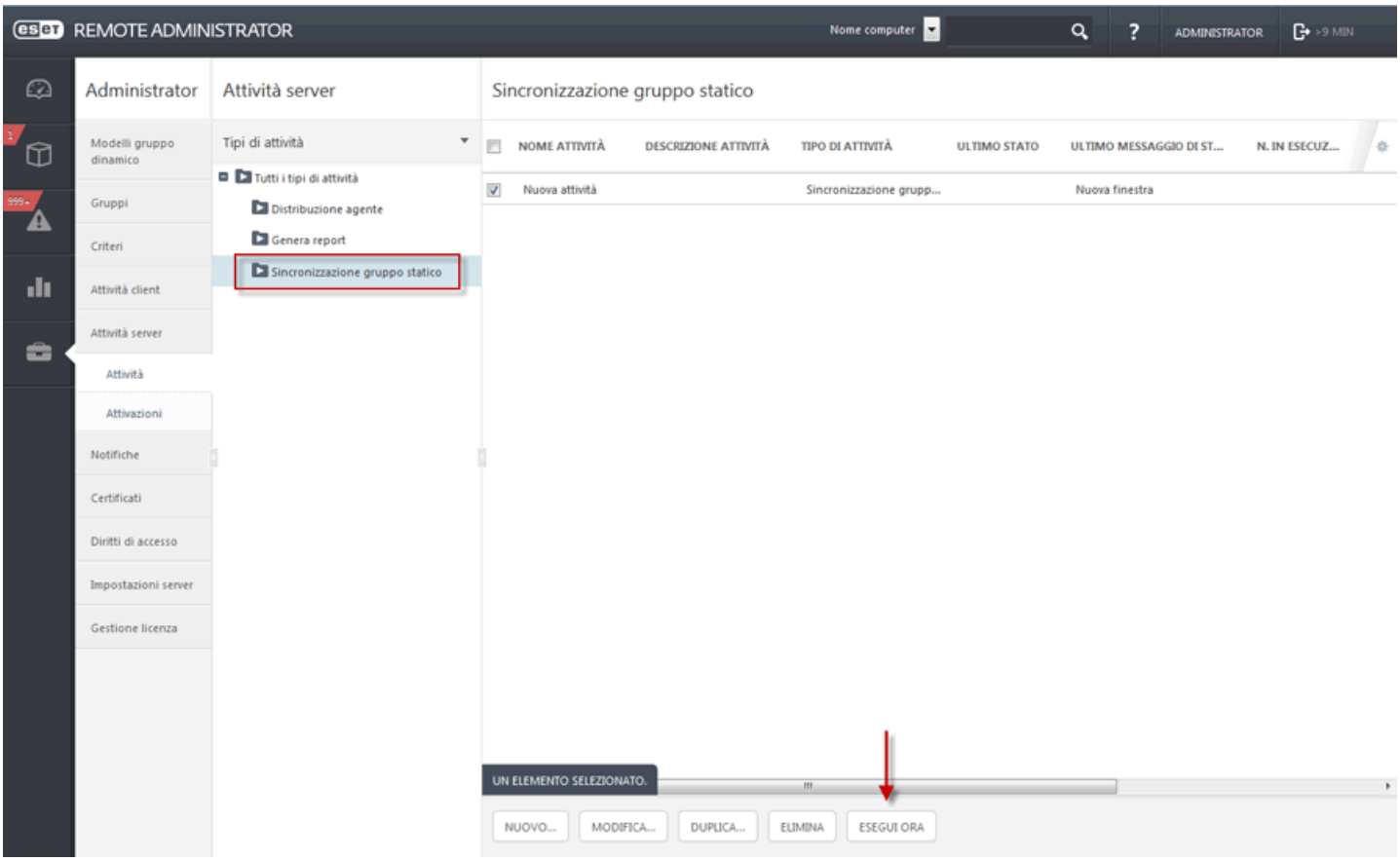
Esistono 3 diversi modi per aggiungere un computer client a ESET Remote Administrator:

- Sincronizzazione Active Directory
- Digitazione manuale nome/IP
- Utilizzo di RD Sensor

4.4.1.1 Utilizzo della sincronizzazione Active Directory

La sincronizzazione AD viene eseguita attraverso il lancio dell'attività del server **Sincronizzazione dei gruppi statici**.

Amministrazione > **Attività server** è un'attività predefinita preimpostata che è possibile scegliere di eseguire automaticamente durante l'installazione di ESET Remote Administrator. Se il computer si trova in un dominio, verrà eseguita la sincronizzazione e i computer provenienti da AD verranno inseriti nel gruppo predefinito **Tutti**.

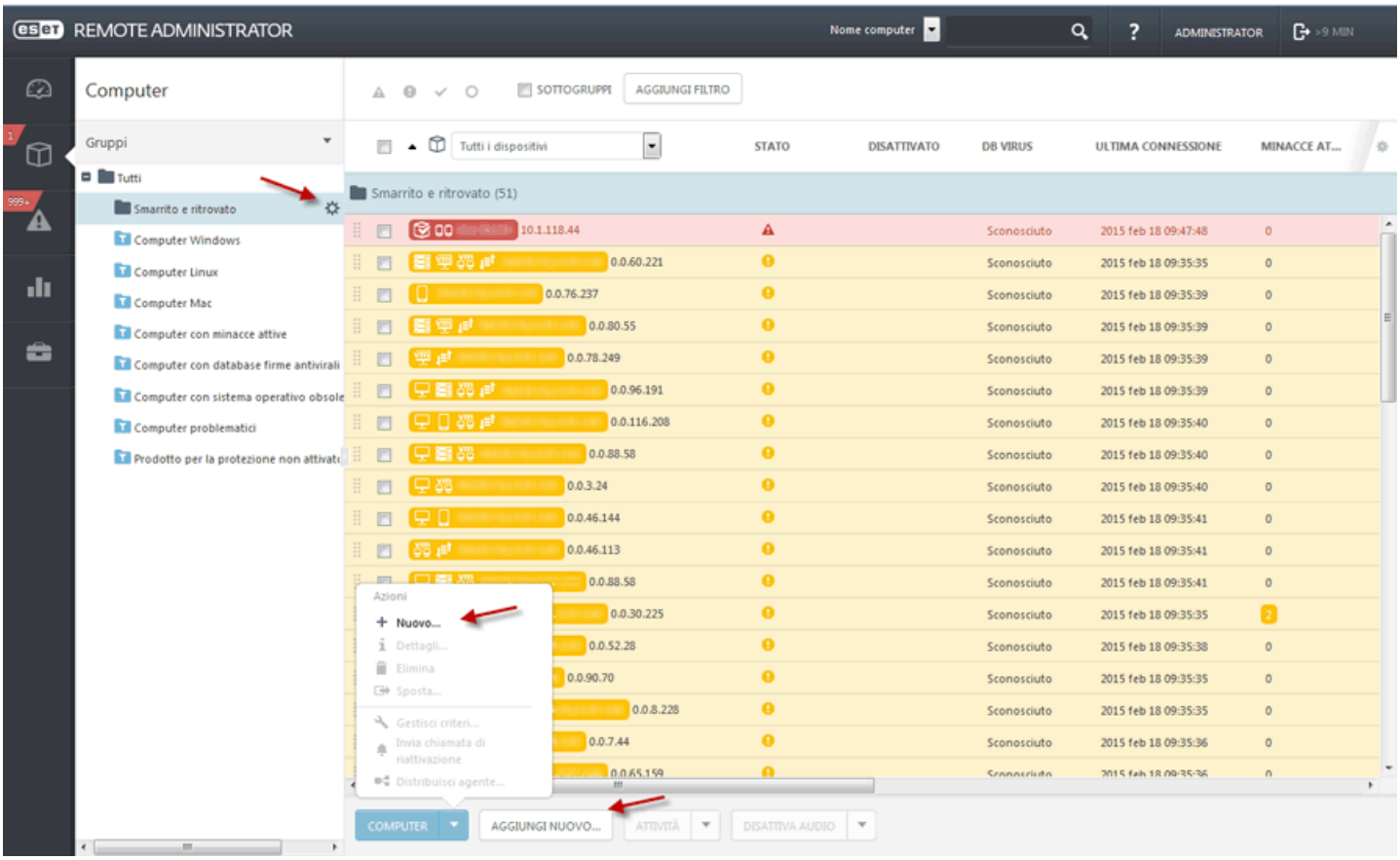


Per avviare il processo di sincronizzazione, basterà fare clic sull'attività e scegliere **Esegui ora**. Se è necessario creare una nuova attività di sincronizzazione AD, selezionare il gruppo al quale aggiungere nuovi computer da AD. Scegliere inoltre gli oggetti nell'AD per i quali eseguire la sincronizzazione e quale azione eseguire per i duplicati. Immettere le impostazioni di connessione del server AD e impostare la **Modalità di sincronizzazione** su **Active Directory/Open Directory/LDAP**.

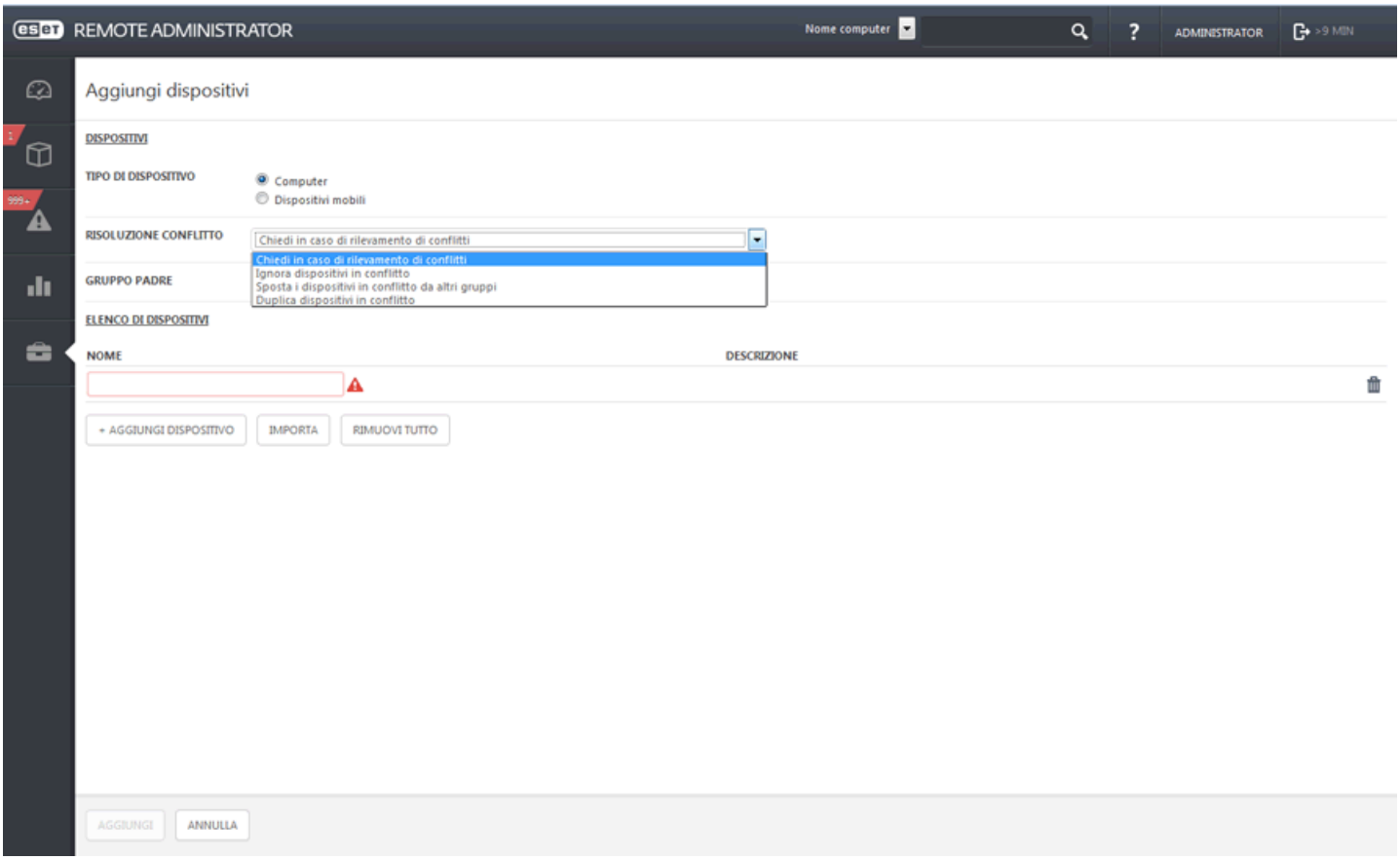
Seguire le istruzioni dettagliate contenute in questo articolo della Knowledge Base ESET.

4.4.1.2 Digitazione manuale nome/IP

La scheda**Computer** consente all'utente di **Aggiungere nuovi** computer. In tal modo, è possibile Aggiungere manualmente computer non trovati o aggiunti automaticamente.



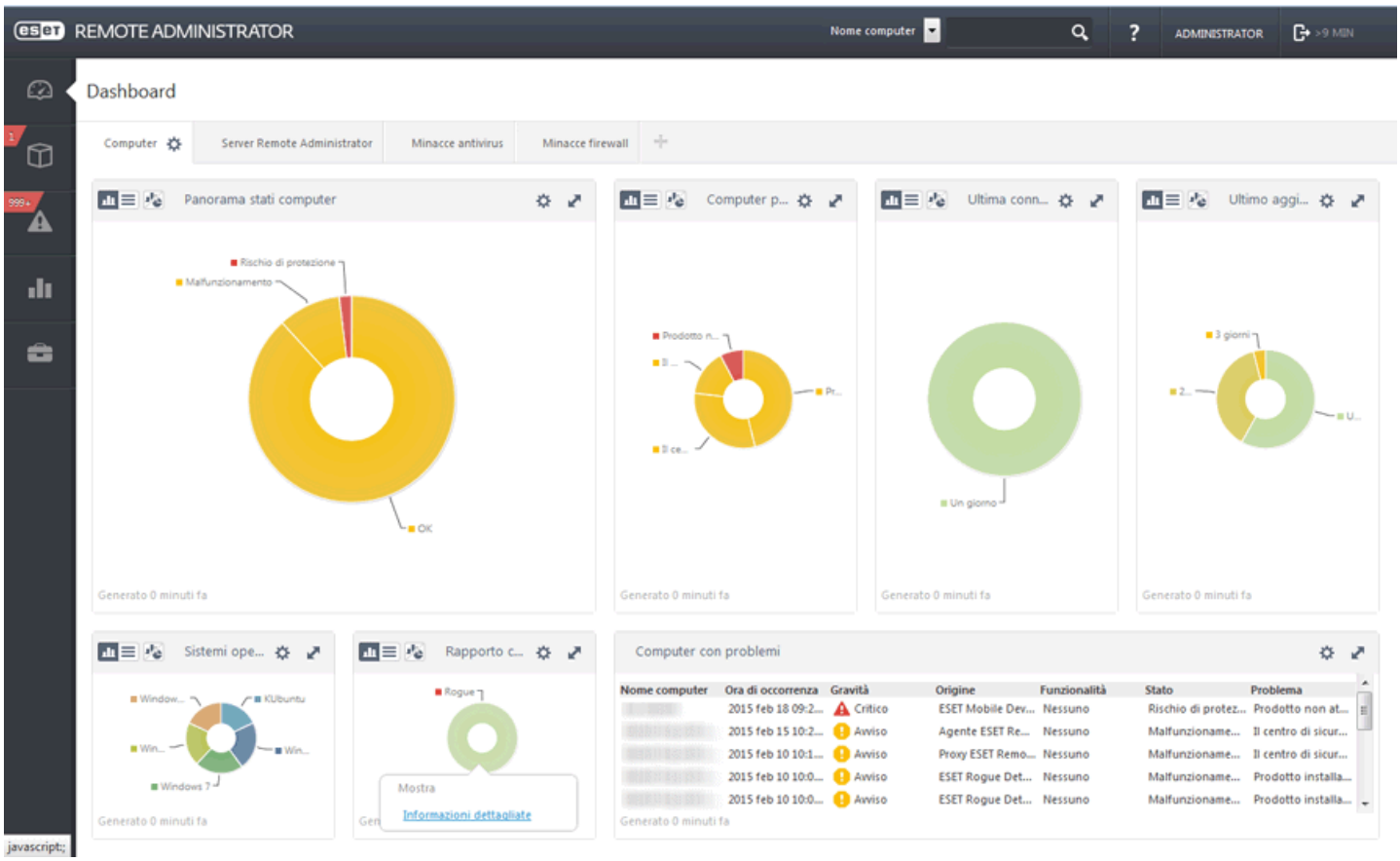
Digitare l'**Indirizzo IP** o il **Nome host** di una macchina che si desidera aggiungere: ESET Remote Administrator ricercherà questi valori nella rete.



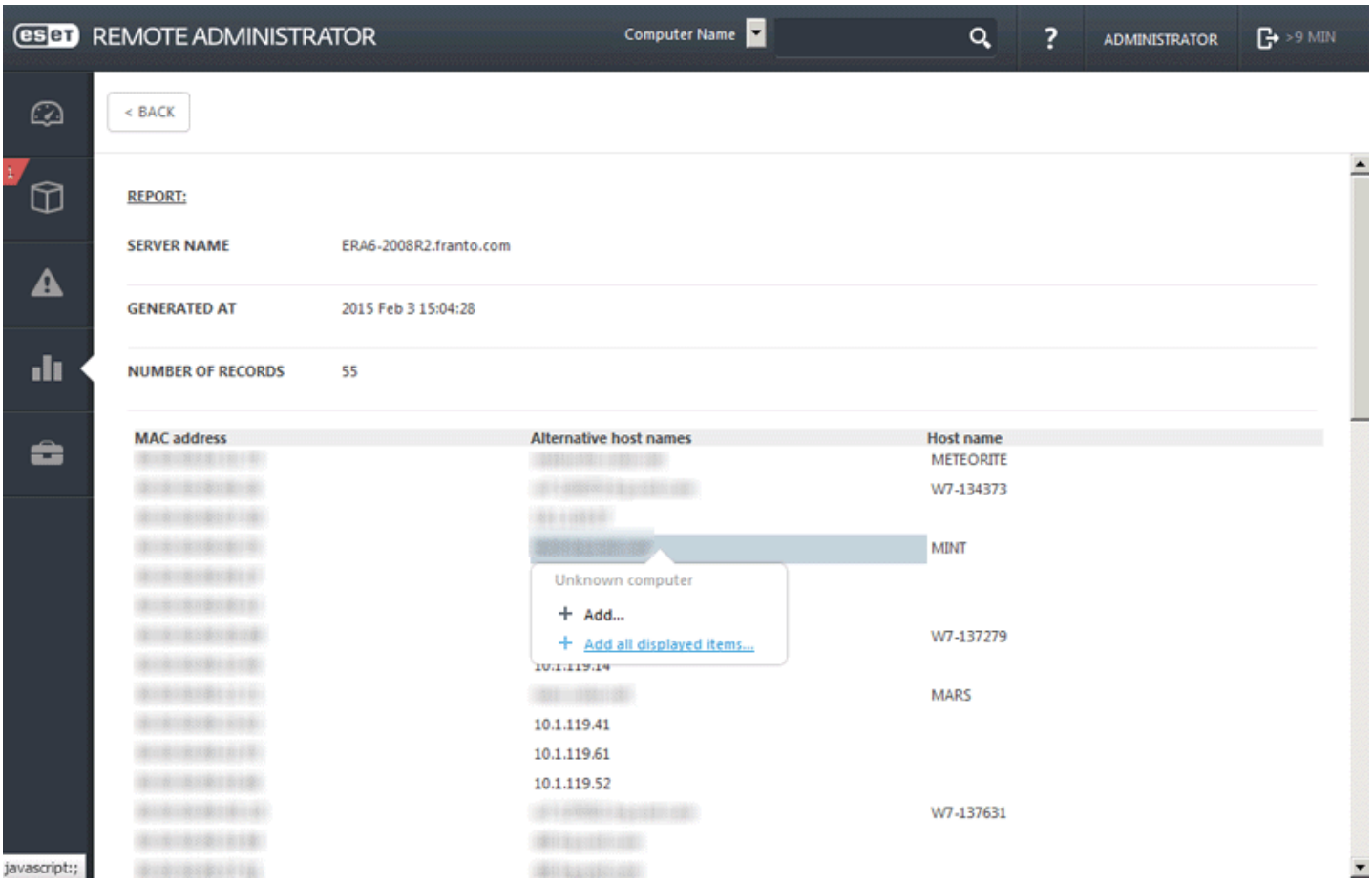
Fare clic su **Aggiungi**. È possibile visualizzare i computer nell'elenco sulla destra dopo aver selezionato il relativo gruppo di appartenenza. Dopo aver aggiunto il computer, si aprirà una finestra popup contenente l'opzione **Distribuisci agente**.

4.4.1.3 Utilizzo di RD Sensor

Se non si utilizza la sincronizzazione AD, il metodo più semplice per aggiungere un computer alla struttura ERA consiste nell'utilizzare l'**RD Sensor**, che rappresenta un componente del bundle di installazione. È possibile eseguire facilmente il drill-down del report **Rapporto computer rogue**, ovvero il grafico in fondo al dashboard Computer, per visualizzare i computer rogue facendo clic sulla parte del grafico di colore rosso.

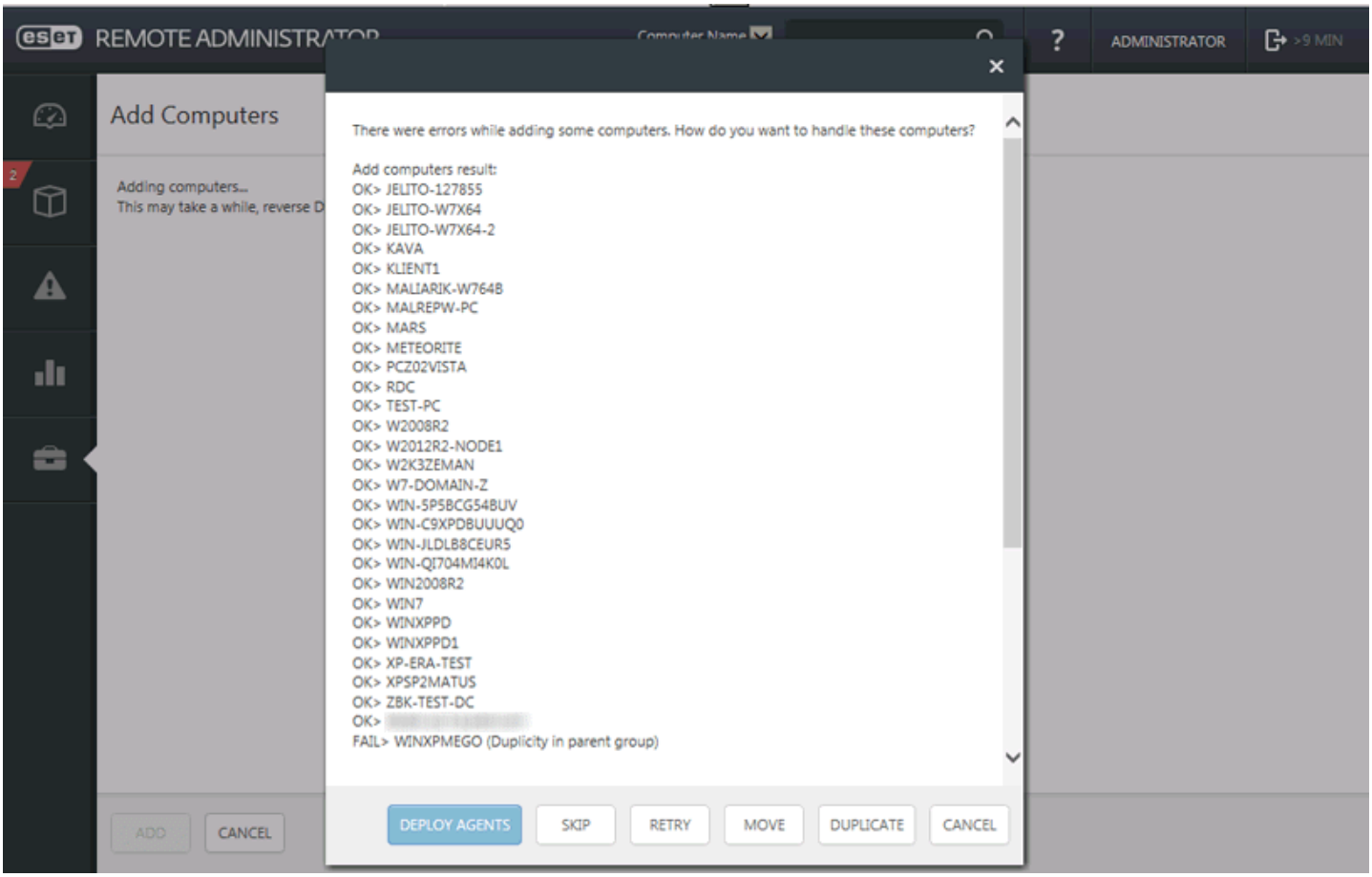


A questo punto, il report dei **Computer Rogue** sul dashboard contiene un elenco dei computer trovati dall'RD Sensor. È ora possibile fare clic sul computer che si desidera **Aggiungere** o **Aggiungere tutti gli elementi visualizzati**.



In caso di aggiunta di un singolo computer, seguire le istruzioni a schermo. È possibile utilizzare un nome precompilato oppure specificarne uno personalizzato (si tratta di un nome visualizzato che verrà utilizzato esclusivamente in ERA Web Console e non di un nome host effettivo). È anche possibile immettere una descrizione facoltativa. Se il computer esiste già nella directory ERA, verrà inviata una notificata all'utente, che potrà decidere cosa fare con il duplicato. Le opzioni disponibili sono: **Distribuisci agente**, **Salta**, **Riprova** , **Sposta**, **Duplica** o **Annulla**. Dopo aver aggiunto il computer, si aprirà una finestra popup contenente l'opzione **Distribuisci agente**.

Se si fa clic su **Aggiungi tutti gli elementi visualizzati**, verrà visualizzato un elenco di computer da aggiungere. Fare clic sulla X accanto al nome di un computer specifico se per il momento non si desidera includerlo nella directory ERA. Al termine della rimozione dei computer dall'elenco, fare clic su Aggiungi. Dopo aver selezionato **Aggiungi**, scegliere l'azione da eseguire quando viene individuato un duplicato (è previsto un leggero ritardo in base al numero di computer presenti nell'elenco): **Salta**, **Riprova**, **Sposta**, **Duplica** o **Annulla**. Dopo aver selezionato un'opzione, si aprirà una finestra popup contenente un elenco di tutti i computer aggiunti che prevede l'opzione **Distribuzione degli agenti** su queste macchine.



I risultati del controllo eseguito dall'RD Sensor vengono scritti in un file di rapporto chiamato `"Macchinerilevate.log"`. contenente un elenco dei computer rilevati sulla rete. Il file `"Macchinerilevate.log"` è disponibile nel seguente percorso:

- Windows
  C:\ProgramData\ESET\Rouge Detection Sensor\Logs
- Linux
  var/log/eset/RemoteAdministrator/RogueDetectionSensor/detectedMachines.log

4.4.2 Distribuzione agente

La distribuzione dell'agente può essere eseguita in modi diversi. L'agente può essere distribuito:

Da remoto, utilizzando un'attività server per la distribuzione di massa dell'agente ERA; in alternativa, è possibile effettuare la distribuzione dell'agente mediante GPO e SCCM
Localmente: attraverso l'utilizzo di un pacchetto di installazione dell'agente o i programmi di installazione live dell'agente, ad esempio se si verificano problemi durante la distribuzione remota

La distribuzione locale può essere eseguita in tre modi:

- Programmi di installazione live dell'agente: attraverso l'utilizzo di uno script generato dall'interno di ERA Web Console, è possibile effettuare la distribuzione dei programmi di installazione live dell'agente tramite e-mail oppure eseguirli da un supporto rimovibile (memoria USB e così via)
- Installazione assistita dal server: attraverso l'utilizzo del pacchetto di installazione dell'agente, i certificati vengono scaricati automaticamente dal server ERA (consigliato metodo di distribuzione locale)
- Installazione off-line: attraverso l'utilizzo del pacchetto di installazione dell'agente, è necessario esportare manualmente i certificati e utilizzarli in questo metodo di distribuzione

L'attività del server relativa alla distribuzione dell'agente da remoto può essere utilizzata per la distribuzione di massa dell'agente ai computer client. Grazie alla possibilità di eseguirlo dalla console Web senza la necessità di distribuire manualmente l'agente su ciascun computer, questo metodo rappresenta la soluzione di distribuzione più appropriata.

Dal momento che le soluzioni di protezione ESET in esecuzione sui computer client comunicano con il server ERA esclusivamente tramite l'agente, l'agente ERA si rivela una risorsa estremamente importante.

NOTA: in caso di problemi con la distribuzione dell'agente ERA da remoto (l'attività server **Distribuzione agente** non riesce), consultare la guida Risoluzione dei problemi.

4.4.2.1 Passaggi distribuzione - Windows

1. Assicurarsi che vengano soddisfatti tutti i **prerequisiti**:

- Il **Server ERA** ed **ERA Web Console** sono installati (su un computer server).
- È stato creato e preparato un certificato **dell'agente** sull'unità locale.
- È stata preparata un'Autorità di certificazione sull'unità locale.
- Il **Computer server** deve essere accessibile dalla rete.

NOTA: in caso di problemi con la distribuzione dell'agente ERA da remoto (l'attività del server **Distribuzione agente** termina con lo stato Non riuscita), consultare la guida Risoluzione dei problemi.

2. Fare doppio clic sul pacchetto di installazione per avviare l'installazione.

3. Inserire un **Host del server** (nome host/indirizzo IP) e una **Porta server** (l'impostazione predefinita è 2222) nei campi appropriati. Questi valori verranno utilizzati per la connessione al server ERA.

4. Selezionare un certificato del peer e una password per il certificato. Facoltativamente, è anche possibile aggiungere un'autorità di certificazione. Questo valore deve essere inserito necessariamente solo per i certificati privi di firma.

5. Selezionare una cartella in cui verrà installato l'**Agente** oppure lasciare selezionata la cartella predefinita.

6. Fare clic su **Installa**. L'**Agente** verrà installato sul computer in uso.

NOTA: qualora sia richiesto un rapporto dettagliato dell'installazione, l'utente dovrà avviare l'installazione attraverso il programma *msiexec* e fornire i parametri richiesti: `msiexec /i program_installer.msi /lv* c:\temp\installer_log.txt`

- La cartella *c:\temp* deve esistere prima dell'esecuzione del comando.

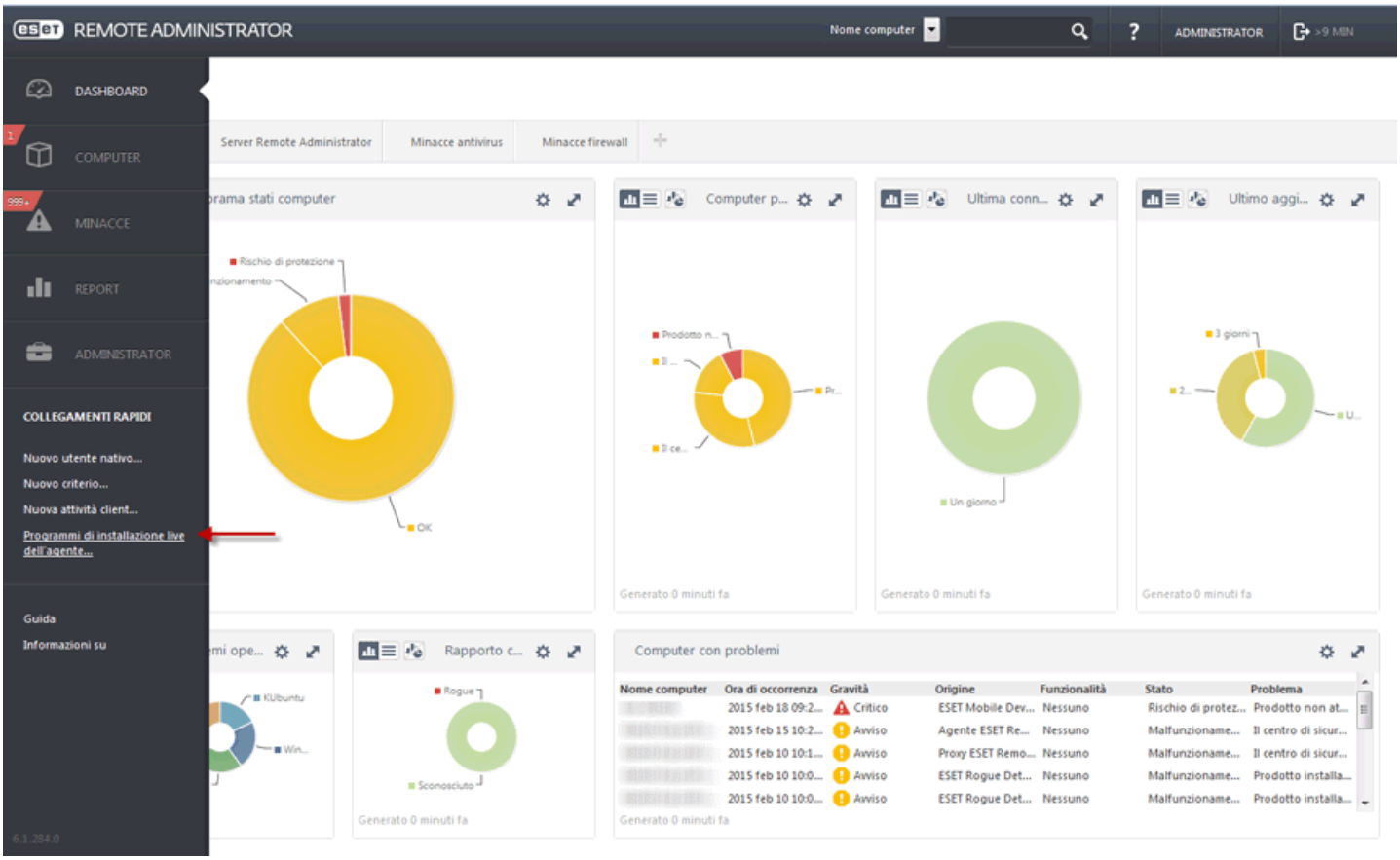
- Per assicurarsi che l'agente ERA funzioni correttamente, controllare il registro di stato sulla macchina client *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*.

4.4.2.1.1 Programmi di installazione live dell'agente

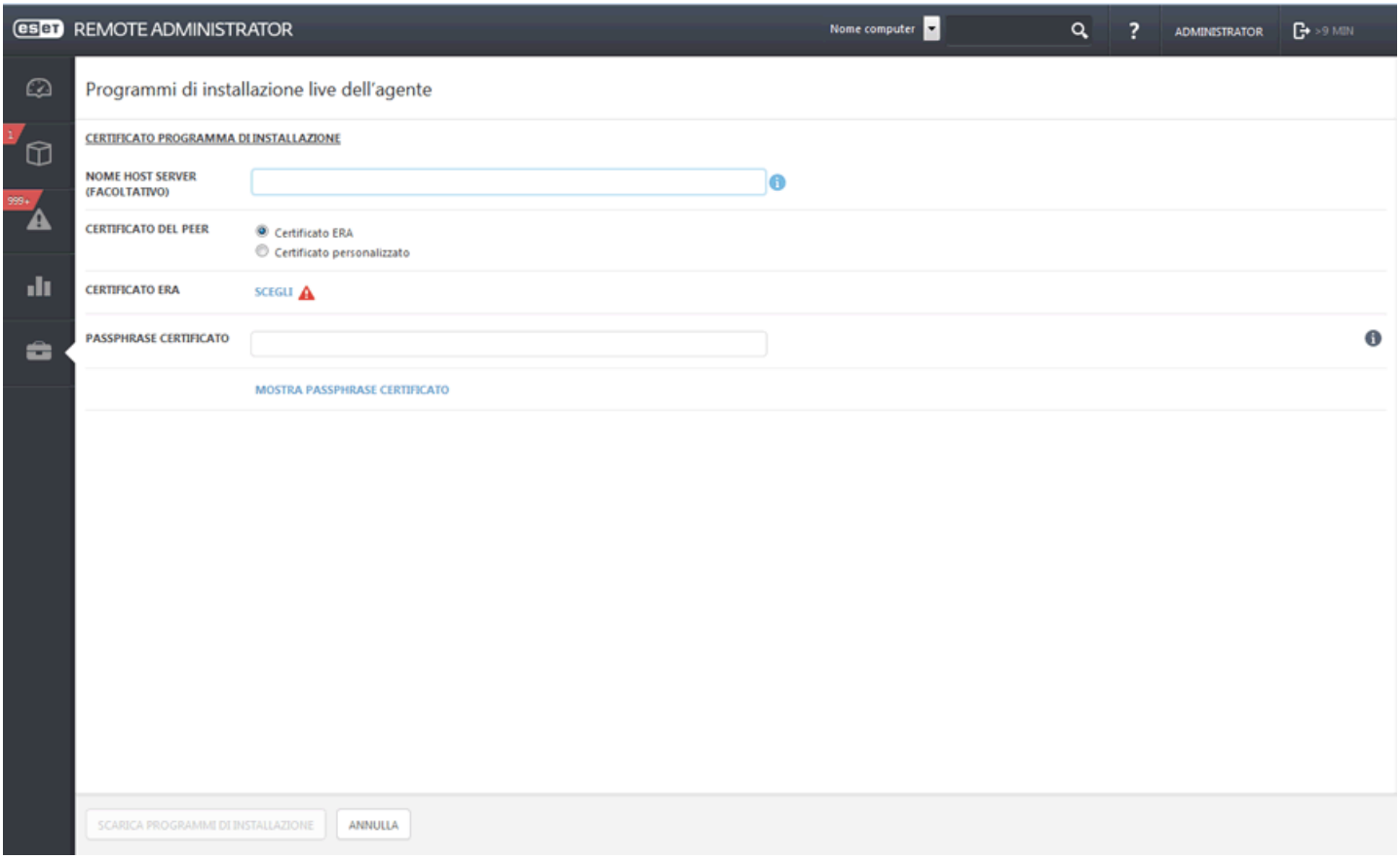
Questo tipo di distribuzione dell'agente risulta utile quando l'opzione di distribuzione locale e da remoto non è adeguata per le esigenze dell'utente. In casi come questo, è possibile effettuare la distribuzione del programma di installazione live dell'agente e consentirne l'utilizzo da parte dell'utente. È anche possibile eseguire il programma di installazione live dell'agente da un supporto rimovibile (memoria USB e così via).

NOTA: è necessario che sulla macchina client sia disponibile una connessione a Internet per scaricare il pacchetto di installazione dell'agente. È inoltre necessario che il client sia in grado di connettersi al server ERA.

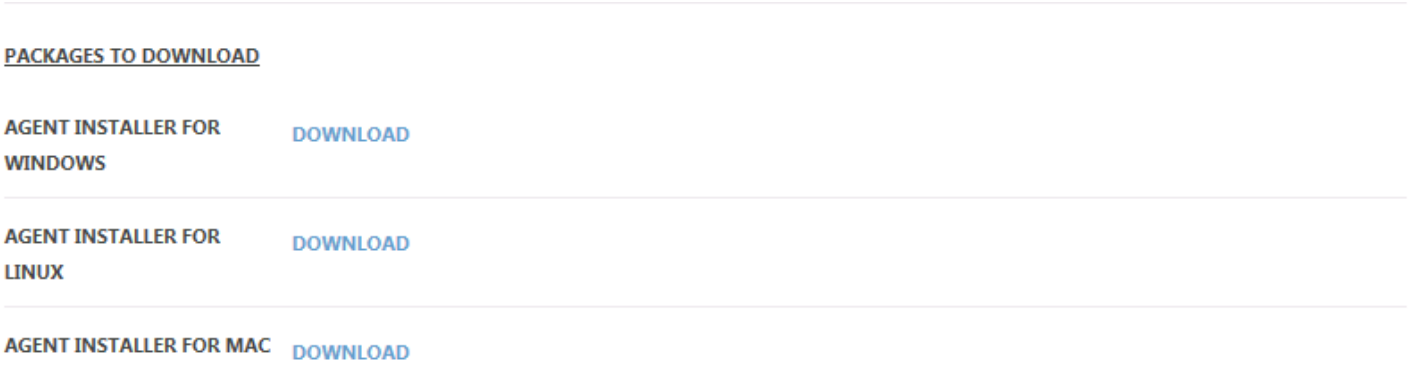
1. Fare clic su **Programmi di installazione live dell'agente...** nella sezione **Collegamenti rapidi** della barra dei menu per creare il programma di installazione.



2. Immettere il nome host del server o l'indirizzo IP e selezionare l'**Autorità di certificazione ERA** creata in fase di installazione iniziale. Immettere la **Passphrase autorità di certificazione** creata durante l'**Installazione del server** quando viene richiesta la password del certificato.



3. Fare clic su **Scarica programmi di installazione** per generare i collegamenti per i file del programma di installazione dell'agente per Windows, Linux e MAC.



4. Fare clic sul collegamento **Download** accanto ai file del programma di installazione che si desidera scaricare e salvare il file **zip**. Decomprimere il file sul computer client sul quale si desidera effettuare la distribuzione dell'agente ERA ed eseguire lo script `EraAgentOnlineInstaller.bat` (Windows) o `EraAgentOnlineInstaller.sh` (Linux e Mac) per eseguire il programma di installazione.

NOTA: se si esegue lo script su Windows XP SP2, è necessario installare il Microsoft Windows Server 2003 Administration Tools Pack. In caso contrario, il programma di installazione live dell'agente non funzionerà correttamente. Dopo aver installato l'Administration Pack, è possibile eseguire lo script del programma di installazione live dell'agente.

Per assicurarsi che l'agente ERA funzioni correttamente, controllare il registro di stato sulla macchina client *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* . In caso di problemi con l'agente, ad esempio se non si connette al server ERA, consultare Risoluzione dei problemi.

Se si desidera effettuare la distribuzione dell'agente ERA mediante il programma di installazione live dell'agente dalla cartella condivisa locale senza ricorrere a ESET Repository Download Server, seguire la procedura sottostante:

1. Modificare il file `EraAgentOnlineInstaller.bat` (Windows) o lo script `EraAgentOnlineInstaller.sh` (Linux e Mac).
2. Modificare le righe 28 e 30 per puntare ai file di download locali corretti. Ad esempio:

```
27
28  set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x64.msi
29  if defined IsArch_x86 (
30    set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x86.msi
31  )
```

3. Utilizzare il proprio URL (al posto di quello visualizzato di seguito):

```
26  )
27
28  set url=\\server\share\Agent_x64.msi
29  if defined IsArch_x86 (
30    set url=\\server\share\Agent_x86.msi
31  )
```

4. Modificare la riga 80 per sostituire " **^& packageLocation ^&** "

```
79  echo.
80  echo.Dim params: params = "/qr /i " ^& packageLocation ^& " /l*v %temp%\ra-agent-install.log" ^&_
```

con **!url!**

```
79  echo.
80  echo.Dim params: params = "/qr /i !url! /l*v %temp%\ra-agent-install.log" ^&_
```

5. **Salvare** il file.

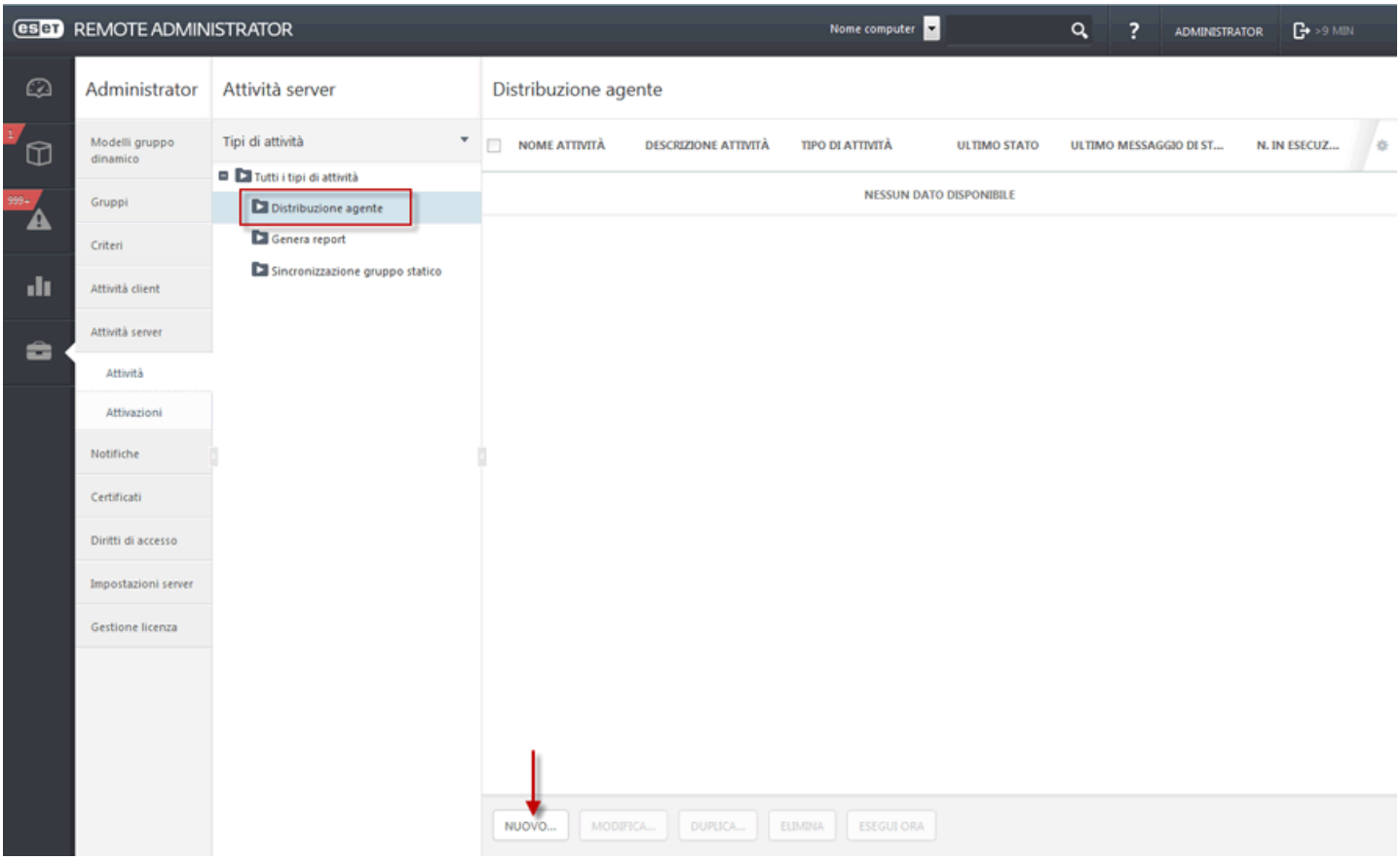
4.4.2.1.2 Distribuisci agente da remoto

Esistono due opzioni per la distribuzione da remoto dell'agente ERA. È possibile utilizzare un'attività server in base a quanto definito di seguito oppure effettuare la distribuzione dell'agente mediante GPO e SCCM.

La distribuzione da remoto dell'agente ERA utilizzando l'attività server viene eseguita dalla sezione **Amministrazione**. Utilizzare le istruzioni che seguono oppure guardare il video illustrativo della Knowledge Base.

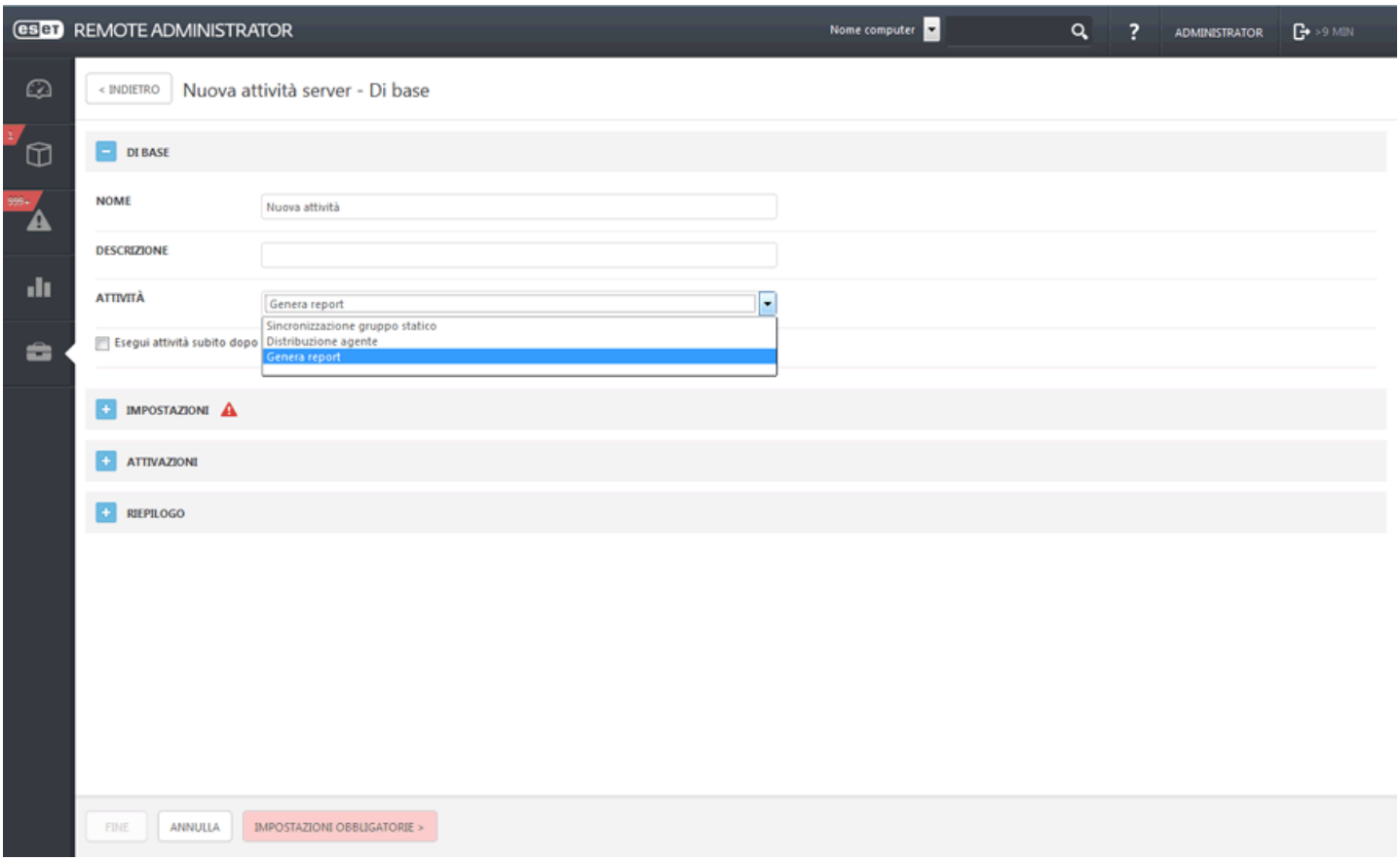
NOTA: si consiglia di testare la distribuzione dell'agente ERA nell'ambiente d'uso prima di utilizzarlo per eseguirne la distribuzione in gruppi di client di grandi dimensioni. Prima di testare la distribuzione di massa, impostare l'Intervallo di connessione dell'agente in base alle proprie preferenze.

Fare clic su **Attività server** > **Distribuzione agente** > **Nuova** per avviare la configurazione della nuova attività.



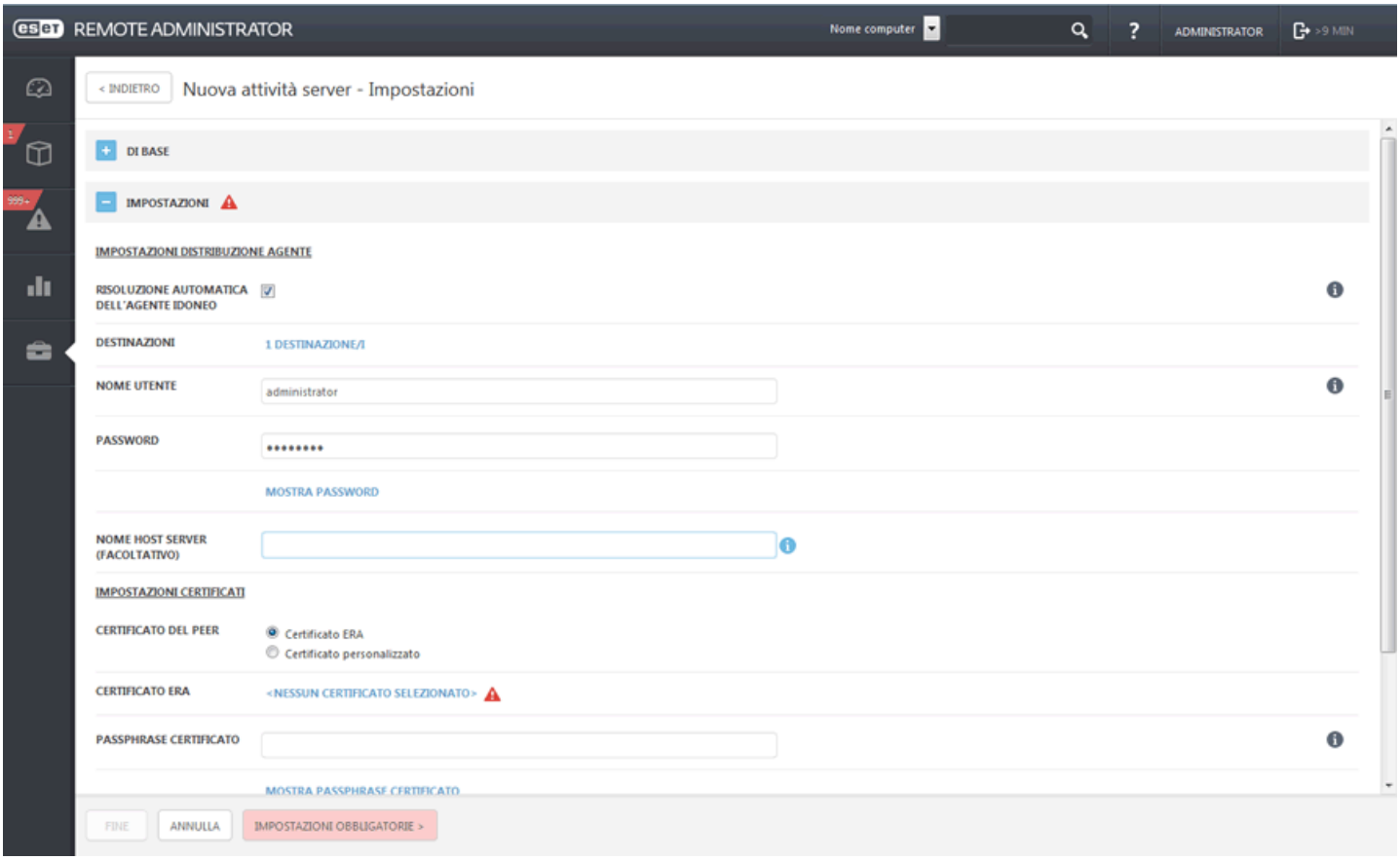
Di base

Inserire le informazioni di base sull'attività, come il **Nome**, la **Descrizione** (facoltativa) e il **Tipo di attività**. Il **Tipo di attività** definisce le impostazioni e il comportamento dell'attività.



Impostazioni

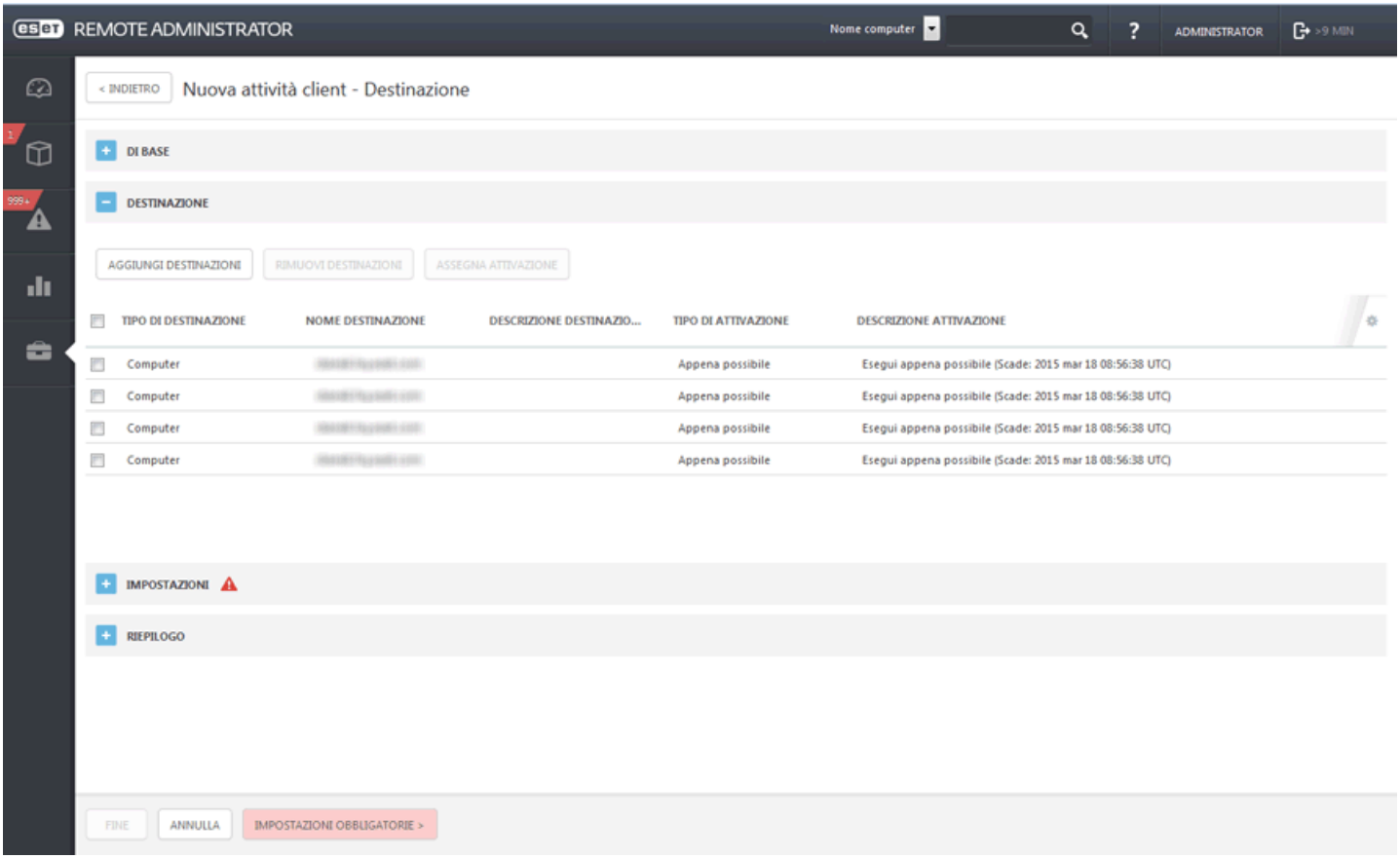
- **Risoluzione automatica dell'agente idoneo**: in presenza di più di un sistema operativo (Windows, Linux, Mac OS) nella rete, dopo aver selezionato questa opzione, l'attività troverà automaticamente il pacchetto di installazione dell'agente appropriato e compatibile con il server per ciascun sistema.
- **Destinazioni**: fare clic per selezionare i client destinatari dell'attività.
- **Nome utente/Password**: nome utente e password dell'utente con diritti sufficienti a eseguire un'installazione remota dell'Agente.
- **Nome host server (facoltativo)**: è possibile inserire un nome host del server, qualora quello sul lato client differisca da quello sul lato server.
- **Certificato del peer/Certificato ERA**: certificato di protezione e autorità di certificazione per l'installazione dell'Agente. È possibile selezionare il certificato predefinito e l'autorità di certificazione oppure utilizzare certificati personalizzati. Per ulteriori informazioni, consultare il capitolo Certificati.
- **Certificato personalizzato**: in caso di utilizzo di un certificato personalizzato per l'autenticazione, accedere al certificato e selezionarlo durante l'installazione dell'agente.
- **Passphrase certificato**: password per il certificato, che corrisponde a quella inserita dall'utente durante l'installazione del server (nel passaggio relativo alla creazione di un'autorità di certificazione) o a quella relativa al certificato personalizzato.



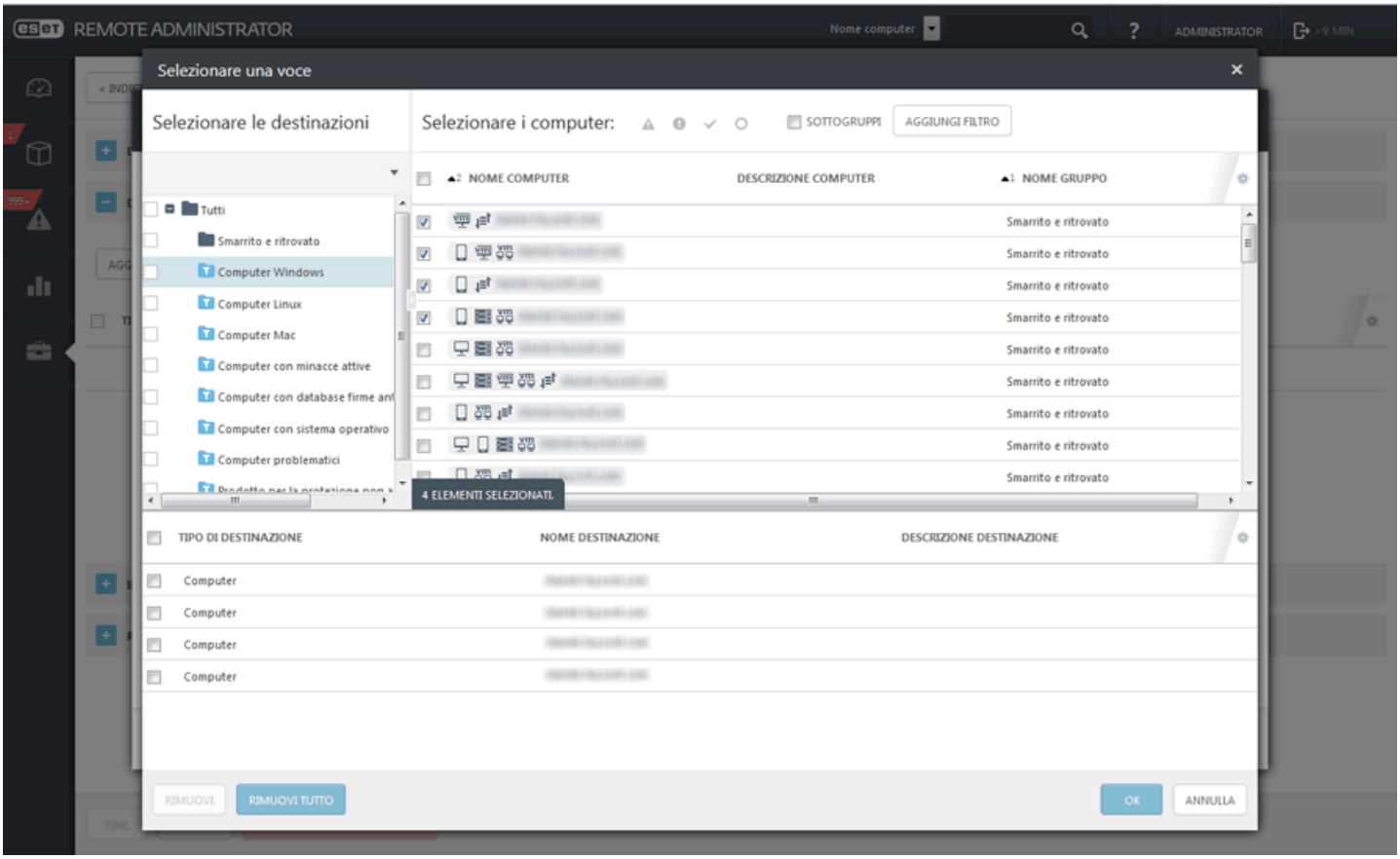
NOTA: il server ERA seleziona automaticamente il pacchetto di installazione dell'agente appropriato per i vari sistemi operativi. Per scegliere manualmente un pacchetto, deselezionare **Risoluzione automatica dell'agente idoneo** e scegliere il pacchetto che si desidera utilizzare nell'elenco di agenti disponibili nell'archivio ERA.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

NOTA: in caso di problemi durante la distribuzione dell'agente ERA da remoto (l'attività del server **Distribuzione agente** non riesce), consultare la sezione Risoluzione dei problemi di questa guida.

4.4.2.1.3 Distribuisci agente localmente

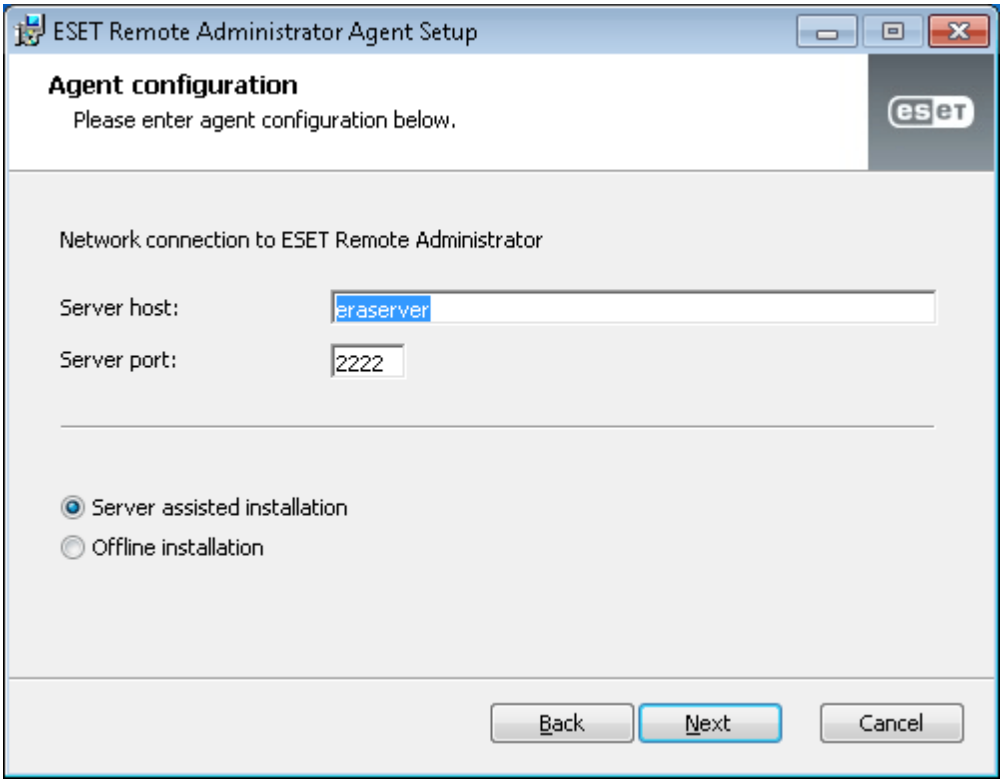
Per distribuire l'agente localmente su un computer cliente tramite la procedura guidata di installazione, seguire i passaggi descritti di seguito:

Scaricare il pacchetto di installazione dell'agente dalla sezione Download del sito Web di ESET sotto a **Gestione remota** (fare clic sul simbolo + per espandere la categoria). Eseguire il programma di installazione sul computer client sul quale si desidera distribuire l'agente. Dopo aver accettato l'EULA, selezionare il tipo di installazione che si desidera eseguire: Installazione assistita dal server o Installazione off-line.

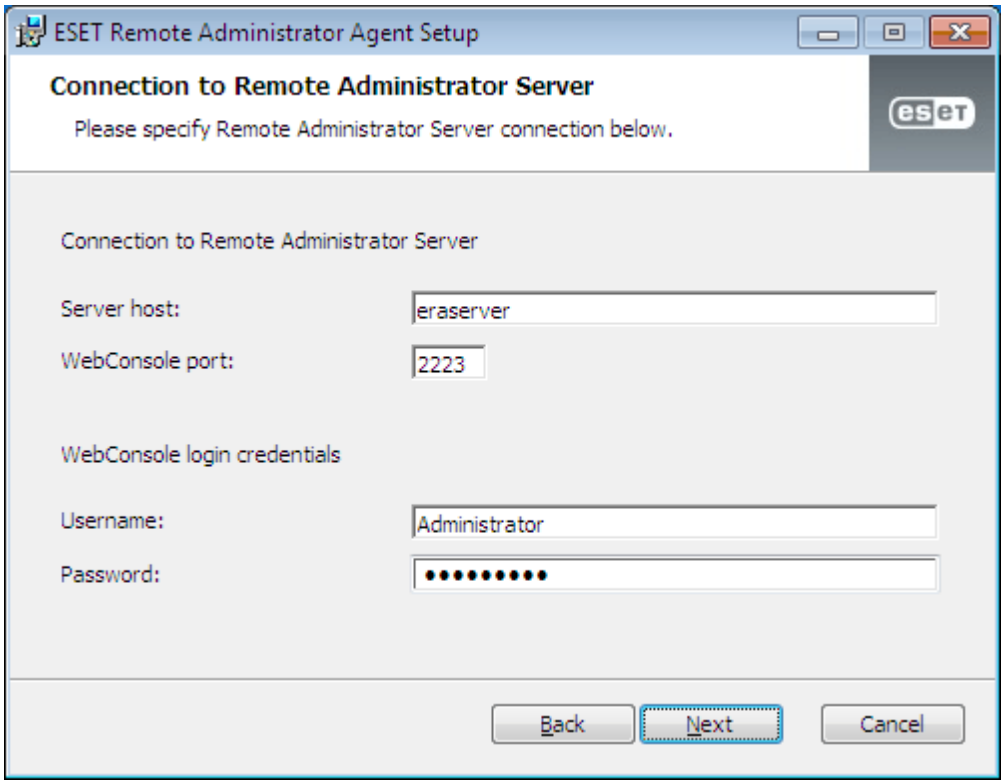
Utilizzare le istruzioni che seguono oppure guardare il video illustrativo della Knowledge Base. È inoltre possibile utilizzare questo articolo della Knowledge Base ESET seguendo le istruzioni dettagliate.

1. **Installazione assistita dal server**:

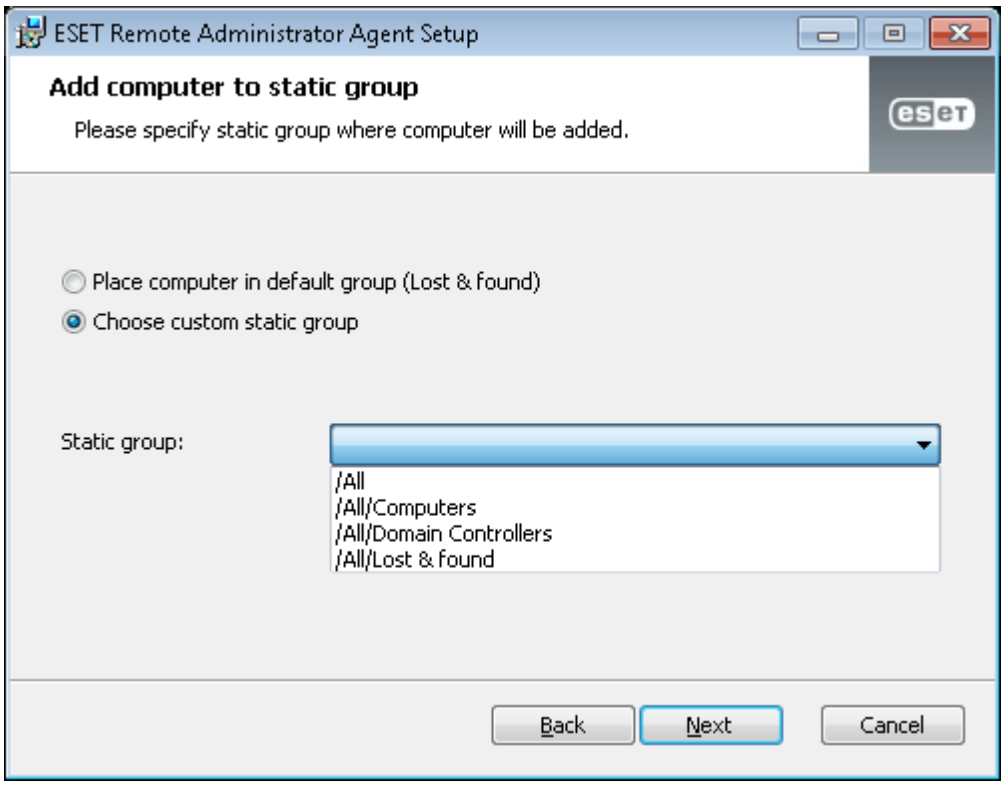
Verificare che l'opzione **Installazione assistita dal server** sia selezionata, specificare l'**Host del server** (nome o indirizzo IP) e la **Porta server** del server ERA, quindi fare clic su **Avanti**. La porta server predefinita è 2222. Se si utilizza una porta differente, sostituire la porta predefinita con il numero di porta personalizzata.



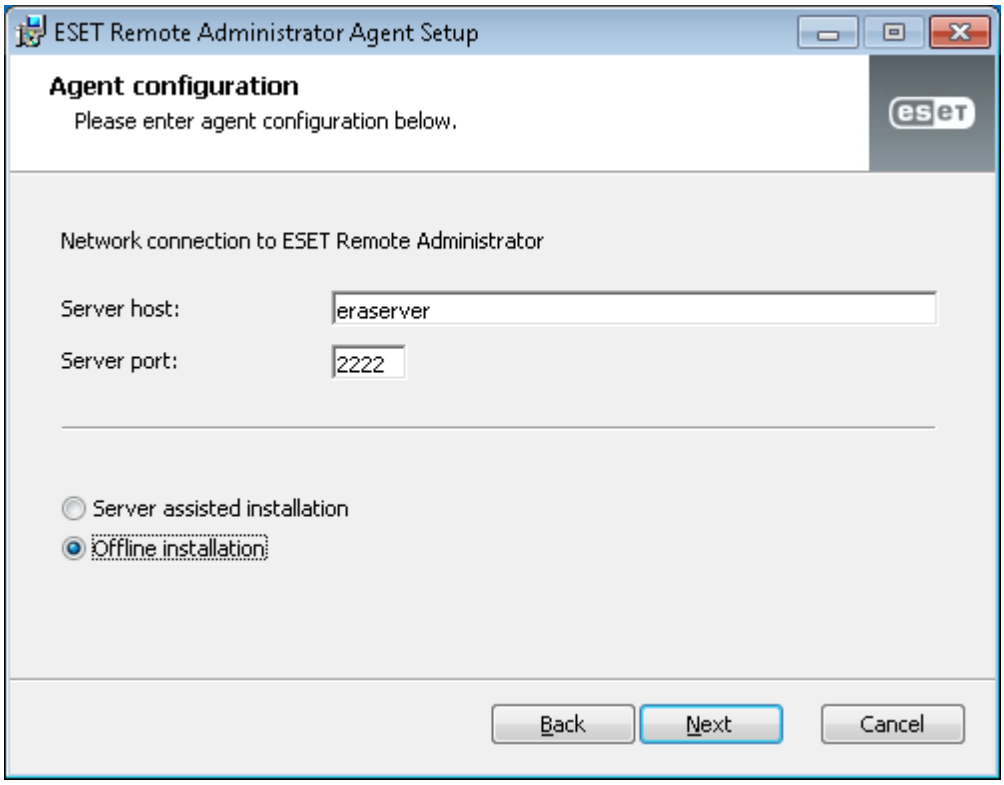
Specificare il metodo utilizzato per la connessione a Remote Administrator Server: il **Server ERA** o **il Server del proxy ERA** e la porta di ERA Web Console, quindi immettere le credenziali di accesso a ERA Web Console: **Nome utente** e **Password**.



Fare clic su **Scegli gruppo statico personalizzato** e selezionare il Gruppo statico al quale sarà aggiunto il computer client tramite il menu a discesa.

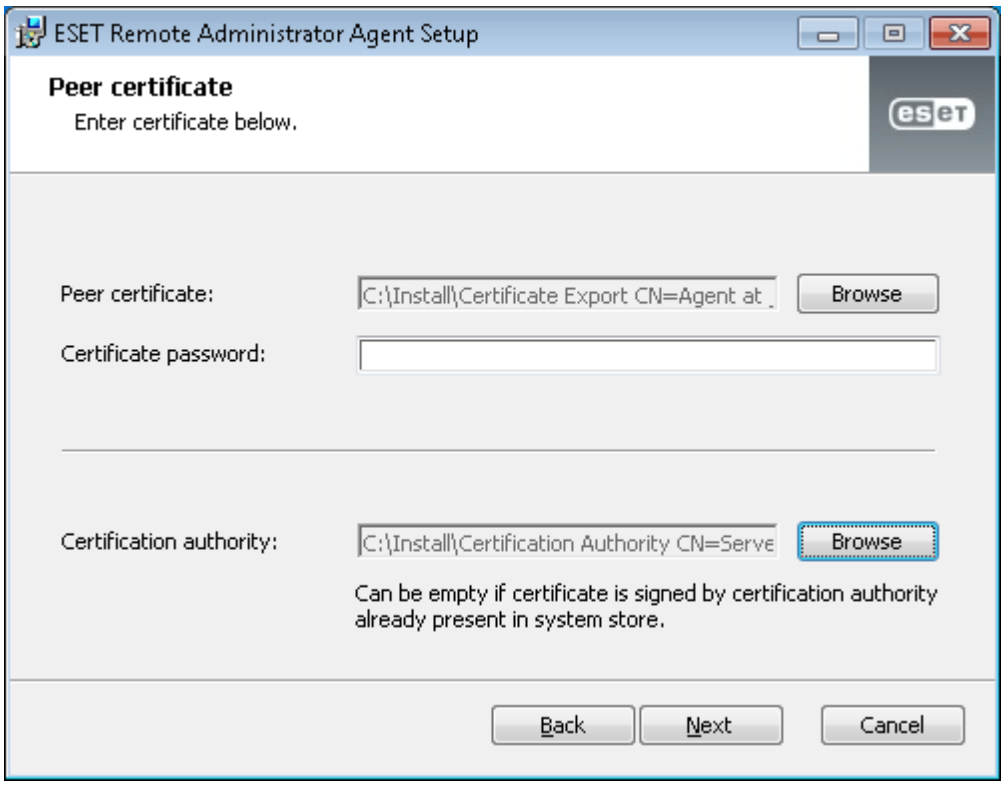


2. **Installazione off-line**:



Per eseguire un'**Installazione off-line**, immettere **2222** nel campo **Porta server**, selezionare **Installazione off-line** e fare clic su **Avanti**. Per utilizzare questo metodo è necessario specificare un **Certificato del peer** e un'**Autorità di certificazione**.

Per ulteriori informazioni sulle modalità di esportazione e di utilizzo di un **Certificato del peer** e di un'**Autorità di certificazione**, fare clic qui.



NOTA: per assicurarsi che l'agente ERA funzioni correttamente, controllare il registro di stato sulla macchina client (in *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html)*. In caso di problemi con l'agente, ad esempio se non si connette al server ERA, consultare il capitolo Risoluzione dei problemi.

4.4.2.2 Passaggi distribuzione - Linux

Questi passaggi si applicano in caso di esecuzione di un'installazione locale dell'agente. Se si desidera utilizzare l'agente su più di un computer, consultare la sezione Distribuzione agente.

Verificare che vengano soddisfatti i seguenti prerequisiti:

- Il server ERA ed ERA Web Console sono installati (su un computer server).
- È stato creato e preparato un certificato dell'agente sull'unità locale.
- È stata preparata l'Autorità di certificazione sull'unità locale.
- Il **Computer server** deve essere accessibile dalla rete.
- Il file di installazione dell'agente deve essere impostato come file eseguibile (chmod +x).

L'agente viene installato mediante l'esecuzione di un comando nel terminale (vedere l'esempio sottostante).

Esempio
(Per facilitare la copia della stringa sul terminale, le nuove righe vengono identificate tramite "\")

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/adminko/Desktop/agent.pfx \
--cert-auth-path=/home/adminko/Desktop/CA.der --cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 --port=2222
```

L'agente ERA e il eraagent.service verranno installati nella seguente posizione:
/opt/eset/RemoteAdministrator/Agent

Parametri di installazione

- *--skip-license* non chiederà all'utente la conferma della licenza.
- *--cert-path* è il percorso che conduce al file del certificato dell'agente.
- *--cert-auth-path* è il percorso che conduce al file dell'autorità di certificazione del server.
- *--cert-password* deve corrispondere alla password del certificato dell'agente
- *--hostname* è una connessione al server (o proxy) in uno dei seguenti formati (nome host, IPv4, IPv6 o record SRV)
- *--port* è una porta di ascolto sia per il server che per il proxy (2222).

Per verificare la correttezza di un'installazione, eseguire il seguente comando:

```
sudo service eraagent status
```

NOTA: se si utilizza un certificato creato dall'utente e firmato da un'autorità diversa dall'Autorità di certificazione ERA, è necessario lasciare il parametro *--cert-auth-path* fuori dallo script di installazione, in quanto l'altra autorità di certificazione è già installata sul sistema operativo Linux (oltre che sul computer server).

NOTA: in caso di problemi durante la distribuzione dell'agente ERA da remoto (l'attività del server **Distribuzione agente** termina con lo stato Non riuscita), consultare la guida Risoluzione dei problemi.

Per assicurarsi che l'agente ERA funzioni correttamente, controllare il registro di stato sulla macchina client */var/log/eset/RemoteAdministrator/Agent/trace.log* o */var/log/eset/RemoteAdministrator/Agent/status.html*.

4.4.2.3 Passaggi di distribuzione - OS X

1. Assicurarsi che vengano soddisfatti tutti i **prerequisiti**:

- Il **Server ERA** ed **ERA Web Console** sono installati (su un computer server).
- È stato creato e preparato un certificato **dell'agente** sull'unità locale.
- È stata preparata un'Autorità di certificazione sull'unità locale.

NOTA: in caso di problemi con la distribuzione dell'agente ERA da remoto (l'attività server **Distribuzione agente** termina con lo stato Non riuscita), consultare la guida Risoluzione dei problemi.

2. Fare doppio clic sul file *.dmg* per avviare l'installazione.
3. Inserire i dati della **Connessione del server**: **Host del server** (nome host o indirizzo IP del server ERA) e **Porta server** (per impostazione predefinita: 2222).
4. Selezionare un certificato del peer e una password per il certificato. Facoltativamente, è anche possibile aggiungere un'autorità di certificazione. Questo valore deve essere inserito necessariamente solo per i certificati privi di firma.
5. Rivedere la posizione dell'installazione e fare clic su **Installa**. L'**Agente** verrà installato sul computer in uso.
6. Il file di rapporto dell'agente ERA è disponibile qui: */Library/Application Support/com.eset.remoteadministrator.agent/Logs/*

4.4.2.4 Risoluzione dei problemi - Distribuzione agente

Durante la fase di distribuzione dell'agente, potrebbero verificarsi alcuni problemi. Le cause di un errore di distribuzione potrebbero essere molteplici. In questa sezione verranno illustrati i seguenti argomenti:

- Trovare le cause dell'insuccesso della distribuzione dell'agente
- Ricercare possibili cause nella tabella sottostante
- Risolvere il problema ed eseguire una corretta distribuzione

Windows

1. Per trovare le cause dell'insuccesso della distribuzione dell'agente, accedere a **Report** > **Automazione**, selezionare **Informazioni sulle attività di distribuzione dell'agente negli ultimi 30 giorni** e fare clic su Genera ora. Verrà visualizzata una tabella contenente informazioni sulla distribuzione. Nella colonna **Avanzamento** vengono visualizzati i messaggi di errore che spiegano il motivo dell'insuccesso della distribuzione dell'agente.

Qualora si desideri avere maggiori dettagli, è possibile modificare il livello di dettaglio del rapporto di monitoraggio del server ERA. Accedere a **Amministrazione** > **Impostazioni server** > **Impostazioni avanzate** > **Registrazione** e selezionare **Errore** dal menu a discesa. Eseguire nuovamente la distribuzione dell'agente e, in caso di errore, ricercare in fondo al file del rapporto di monitoraggio del server ERA le voci più recenti. Il report includerà alcuni suggerimenti sulle modalità di risoluzione del problema. Il file di rapporto più recente del server ERA è disponibile qui: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*

Per attivare la registrazione completa, creare un file fittizio chiamato **traceAll** senza estensione nella stessa cartella di un trace.log. Riavviare il servizio ESET Remote Administrator Server per attivare la registrazione completa nel file **trace.log**.

2. Nella tabella sottostante sono riportati alcuni motivi dell'insuccesso della distribuzione dell'agente:

Messaggio di errore	Possibile causa
Impossibile stabilire la connessione	Il client non è raggiungibile sulla rete Non è possibile risolvere il nome host del client Il firewall blocca le comunicazioni Le porte 2222 e 2223 non sono aperte nel firewall (sia sul lato client sia sul lato server)
Accesso negato	Nessuna password impostata per l'account di amministratore Diritti di accesso insufficienti La condivisione amministrativa ADMIN$ non è disponibile La condivisione amministrativa IPC$ non è disponibile È stato attivato l'utilizzo della condivisione semplice dei file
Pacchetto non trovato nell'archivio	Il collegamento all'archivio non è corretto L'archivio non è disponibile L'archivio non contiene il pacchetto richiesto

3. Seguire la procedura appropriata per la risoluzione dei problemi in base alla possibile causa:

- Il client non è raggiungibile sulla rete: effettuare il ping del client dal server ERA e, in caso di risposta, tentare di accedere da remoto alla macchina client (ad esempio attraverso il desktop remoto).
- Non è possibile risolvere il nome host del client: le possibili soluzioni ai problemi del DNS includono, ad esempio:

  Utilizzo del comando `nslookup` comando dell'indirizzo IP e del nome host del server e/o dei client con problemi di distribuzione dell'agente. I risultati dovrebbero corrispondere alle informazioni della macchina. Ad esempio, un `nslookup` di un nome host dovrebbe risolversi in un indirizzo IP; un comando `ipconfig` viene visualizzato sull'host in questione. Il comando `nslookup` dovrà essere eseguito sui client e sul server.

  Ricerca manuale di duplicati nei record del DNS.
- Il firewall blocca le comunicazioni: controllare le impostazioni del firewall sia sul lato server sia sul lato client, nonché altri firewall esistenti tra le due macchine (se applicabile).
- Le porte 2222 e 2223 non sono aperte nel firewall: valgono le stesse condizioni di cui sopra. Assicurarsi che le porte siano aperte su tutti i firewall tra le due macchine (client e server).
- Nessuna password impostata per l'account di amministratore: impostare una password corretta per l'account di amministratore (non utilizzare password vuote)
- Diritti di accesso insufficienti: tentare di utilizzare le credenziali dell'amministratore di dominio durante la creazione di un'attività di distribuzione dell'agente. Se la macchina client è posizionata in un gruppo di lavoro, utilizzare l'account di amministratore locale su quella specifica macchina.
- La condivisione amministrativa ADMIN$ non è disponibile: sulla macchina client è necessario attivare la risorsa condivisa ADMIN$. Assicurarsi che tale risorsa sia presente tra le altre condivisioni (**Start** > **Pannello di controllo** > **Strumenti di amministrazione** > **Gestione computer** > **Cartelle condivise** > **Condivisioni**).
- La condivisione amministrativa IPC$ non è disponibile: verificare che il client abbia accesso all'IPC, attivando il seguente comando da un prompt dei comandi sul client:

  ```
  utilizzo rete \\servername\IPC$
  ```

  dove *servername* è il nome del server ERA

- È stato attivato l'utilizzo della condivisione semplice dei file: nel caso in cui compaia il messaggio di errore "Accesso negato" e sia presente un ambiente misto (formato da un dominio e un gruppo di lavoro), disattivare **Utilizza condivisione semplice dei file** oppure **Utilizza procedura guidata condivisione** su tutte le macchine che riscontrano problemi con la distribuzione dell'agente. Ad esempio, in Windows 7, seguire la procedura sottostante:
  - Fare clic su **Start**, digitare `cartella` nella casella di ricerca, quindi fare clic su **Opzioni cartella**. Fare clic sulla scheda **Visualizza** e nella casella Impostazioni avanzate scorrere l'elenco e deselezionare la casella di controllo accanto a **Utilizza procedura guidata condivisione**.

- Il collegamento all'archivio non è corretto: in ERA Web Console, accedere ad **Amministrazione** > **Impostazioni server,** fare clic su **Impostazioni avanzate** > **Archivio** e assicurarsi che l'indirizzo URL dell'archivio sia corretto.
- Pacchetto non trovato nell'archivio: in genere questo messaggio di errore viene visualizzato quando non è presente alcuna connessione all'archivio ERA. Controllare la connessione a Internet.

NOTA: per i sistemi operativi più recenti di Windows (Windows 7, Windows 8, ecc.), è necessario attivare l'account utente Amministratore per poter eseguire l'attività di distribuzione dell'agente.

Per attivare l'account utente Amministratore:
1. Aprire un prompt dei comandi amministrativo
2. Inserire il seguente comando: `amministratore utente rete /attivo:sì`

Linux e Mac OS

Se la distribuzione dell'agente non funziona su Linux o Mac OS, nella maggior parte dei casi si tratta di un problema correlato all'SSH. Controllare il computer client e assicurarsi che il daemon SSH sia in esecuzione. Dopo aver risolto il problema, eseguire nuovamente la distribuzione dell'agente.

4.4.3 Distribuzione dell'agente mediante GPO e SCCM

Dopo aver installato correttamente ESET Remote Administrator, è necessario effettuare la distribuzione dell'**Agente ERA**e **dei prodotti di protezione** ESET sui computer client presenti nella rete.

Oltre alla distribuzione locale o da remoto mediante l'utilizzo di un'attività server, è possibile utilizzare strumenti di gestione quali GPO, SCCM, Symantec Altiris o Puppet. Fare clic sul collegamento appropriato in basso per visualizzare le istruzioni dettagliate relative a due metodi comuni di distribuzione dell'agente ERA:

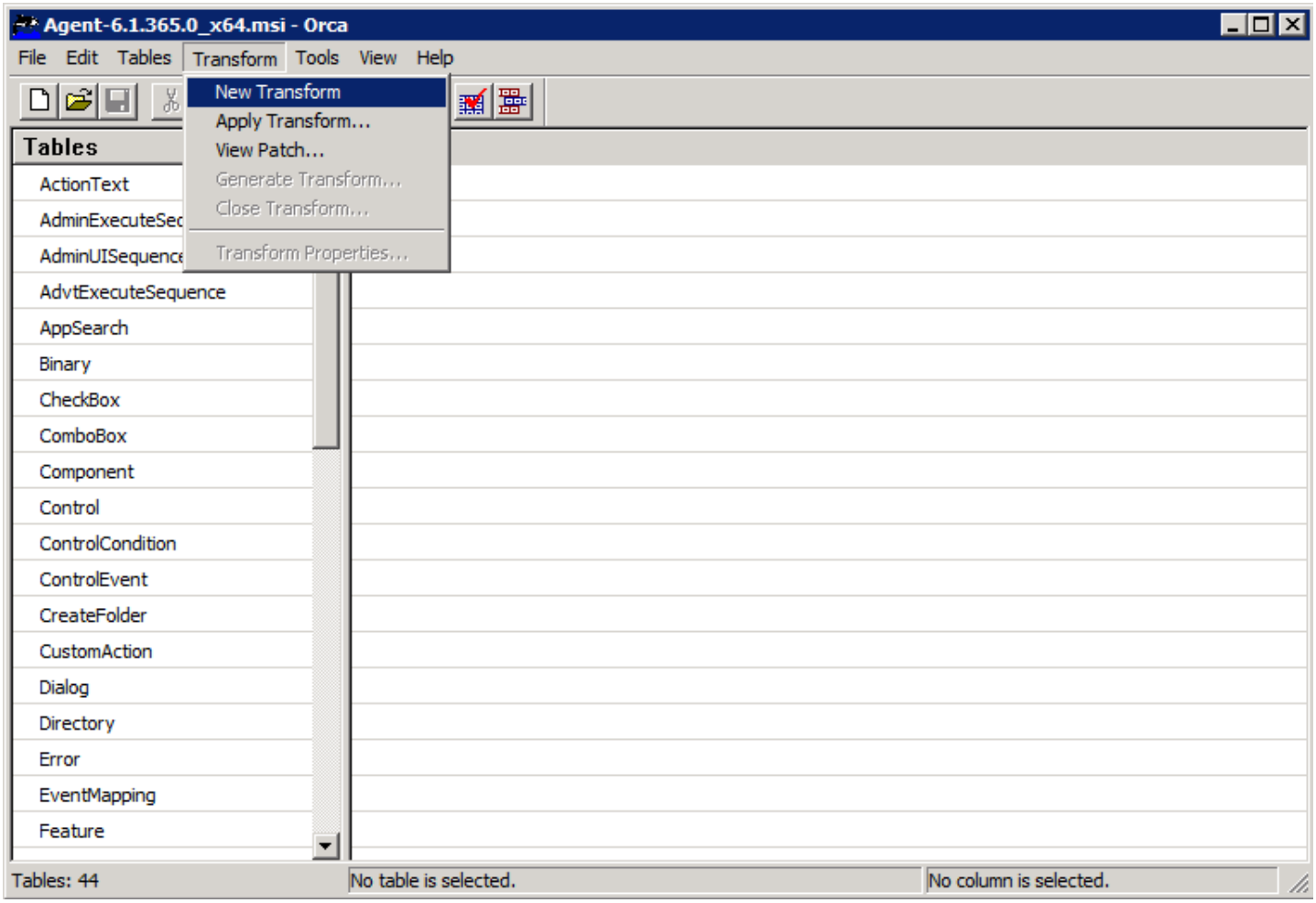
1. Distribuzione dell'agente ERA mediante GPO
2. Distribuzione dell'agente ERA mediante SCCM

4.4.3.1 Creare il file MST

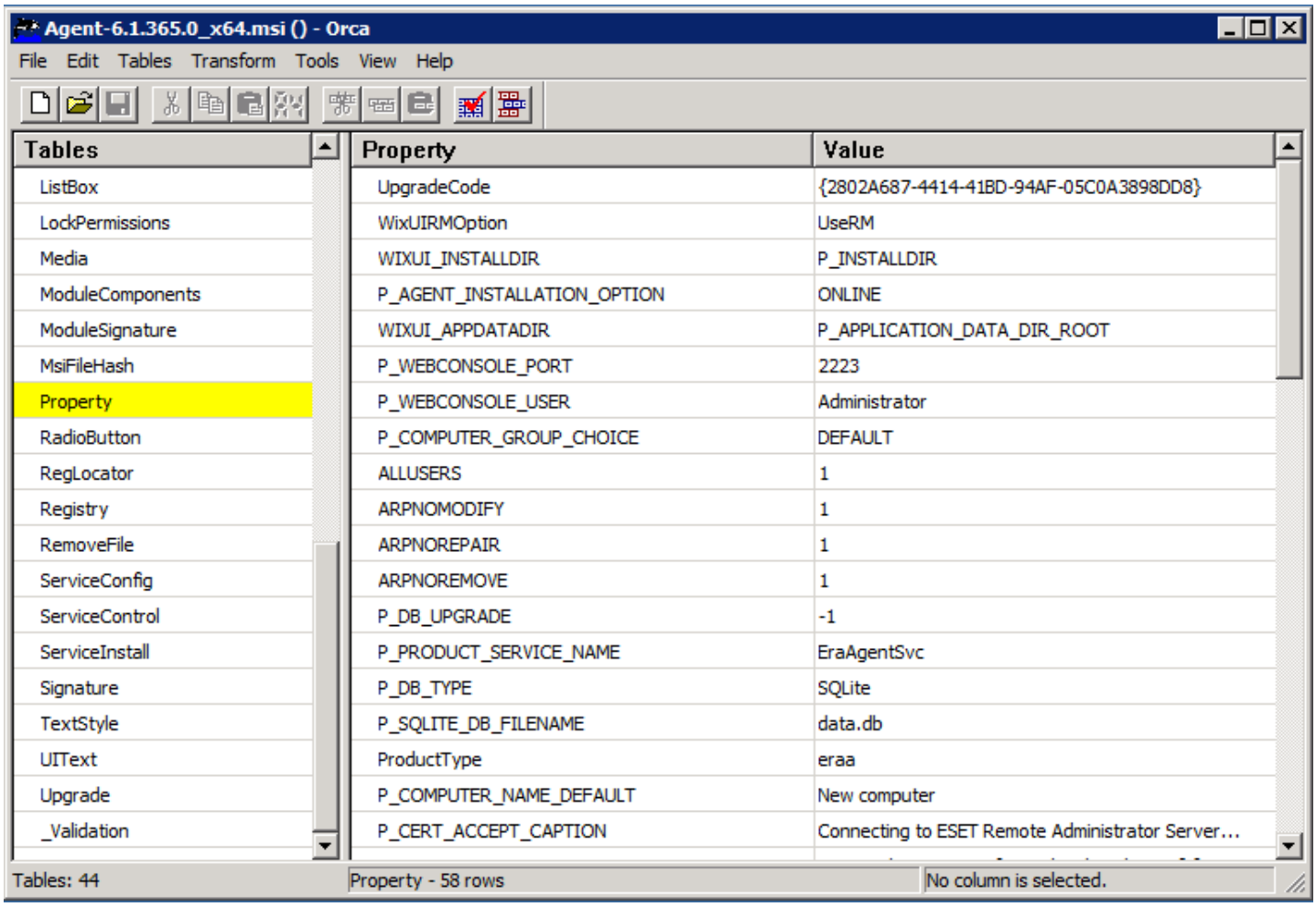
Prima di eseguire la distribuzione del file del programma di installazione dell'agente ERA, è necessario creare un file di trasformazione `.mst` con le impostazioni per l'agente ERA. Per creare un file di trasformazione, seguire la procedura sottostante oppure consultare questo articolo della Knowledge Base.

1. Installare Orca (parte di Windows SDK). Per ulteriori informazioni su Orca, consultare http://support.microsoft.com/kb/255905/
2. Scaricare il programma di installazione dell'**Agente ERA**. Ad esempio, è possibile utilizzare `Agent-6.1.365.0_x64.msi`, che è un componente di ERA versione 6.1.28.0 per i sistemi a 64 bit. Per un elenco delle versioni dei componenti ERA, consultare il relativo articolo della Knowledge Base.
3. Aprire Orca facendo clic su Start > **Tutti i programmi** > **Orca**.

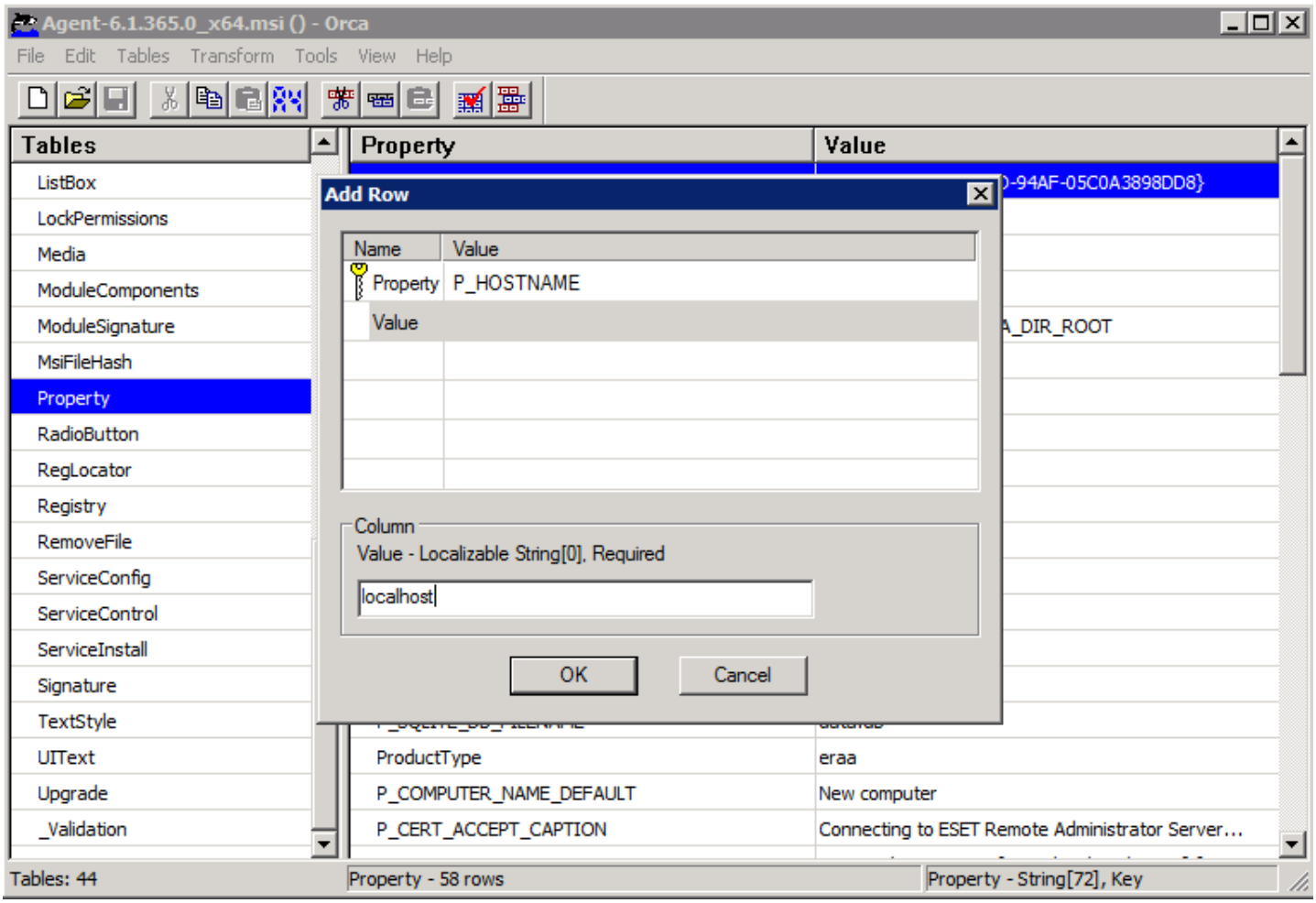
4. Fare clic su **File** nel menu in alto, quindi su **Apri** e ricercare il file `Agent-6.1.365.0_x64.msi`.
5. Fare clic su **Trasforma** nel menu in alto e selezionare **Nuova trasformazione**.



6. Fare clic su **Proprietà**.



7. Fare clic con il pulsante destro del mouse in un punto qualsiasi dell'elenco dei valori delle proprietà e selezionare **Aggiungi riga** dal menu contestuale.
8. Aggiungere la proprietà **P_HOSTNAME** e digitare il nome host o l'indirizzo IP del server ERA nel campo **Valore**.
9. Ripetere i passaggi 7 e 8 per aggiungere la proprietà P_PORT, dove, per impostazione predefinita, il valore è rappresentato dalla porta utilizzata per effettuare la connessione al server ERA (2222).

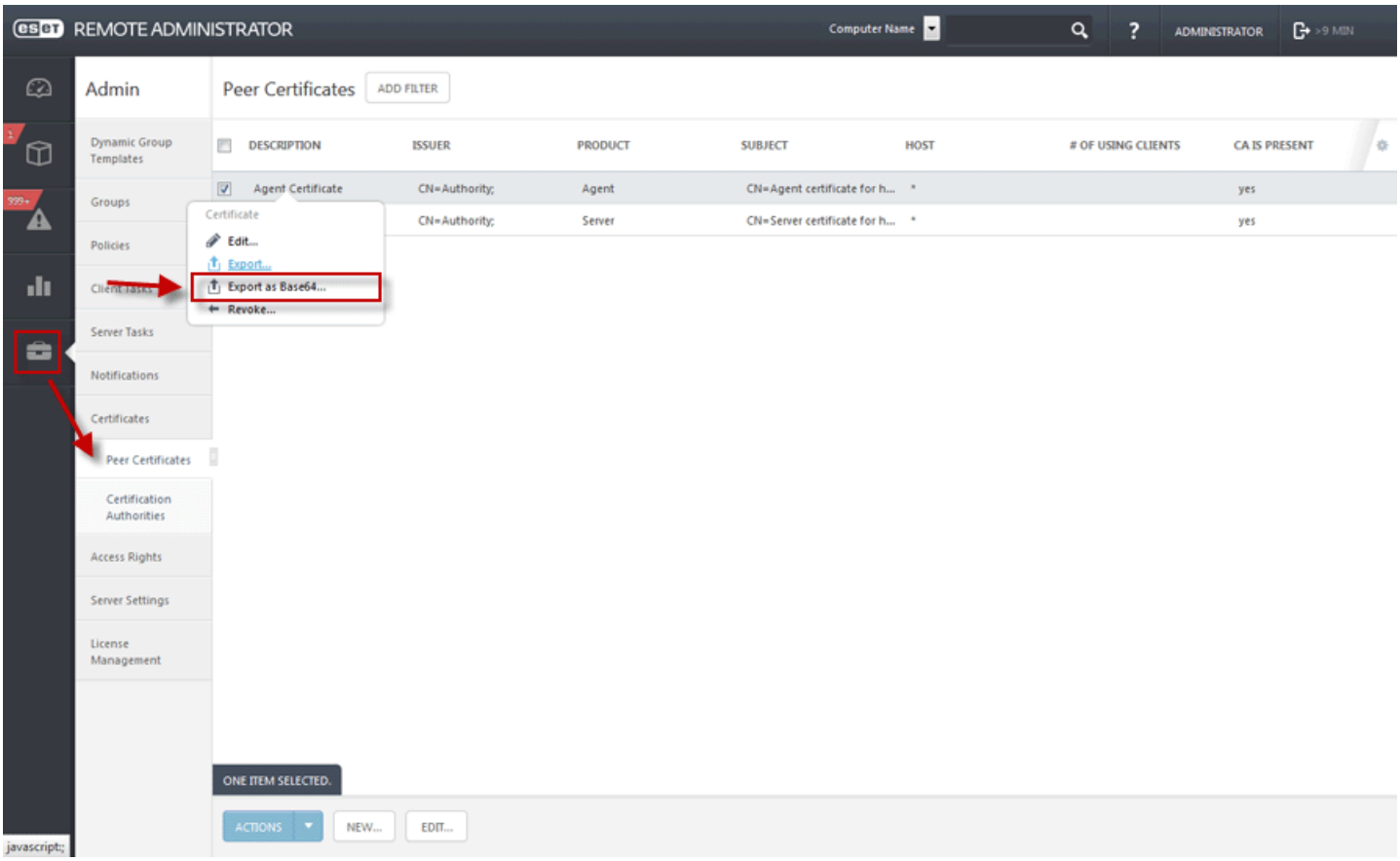


10. Per l'agente ERA, inserire il certificato del peer (.pfx) firmato dall'autorità di certificazione archiviata nel database del server ERA. Inserire la chiave pubblica dell'autorità di certificazione (file `.der`) utilizzata per la firma del certificato del peer del server ERA.

- **Esistono due modi per inserire i certificati:**

1. È possibile inserire i contenuti del certificato e della chiave pubblica codificata in **Formato Base64** (non saranno necessari file di certificati).

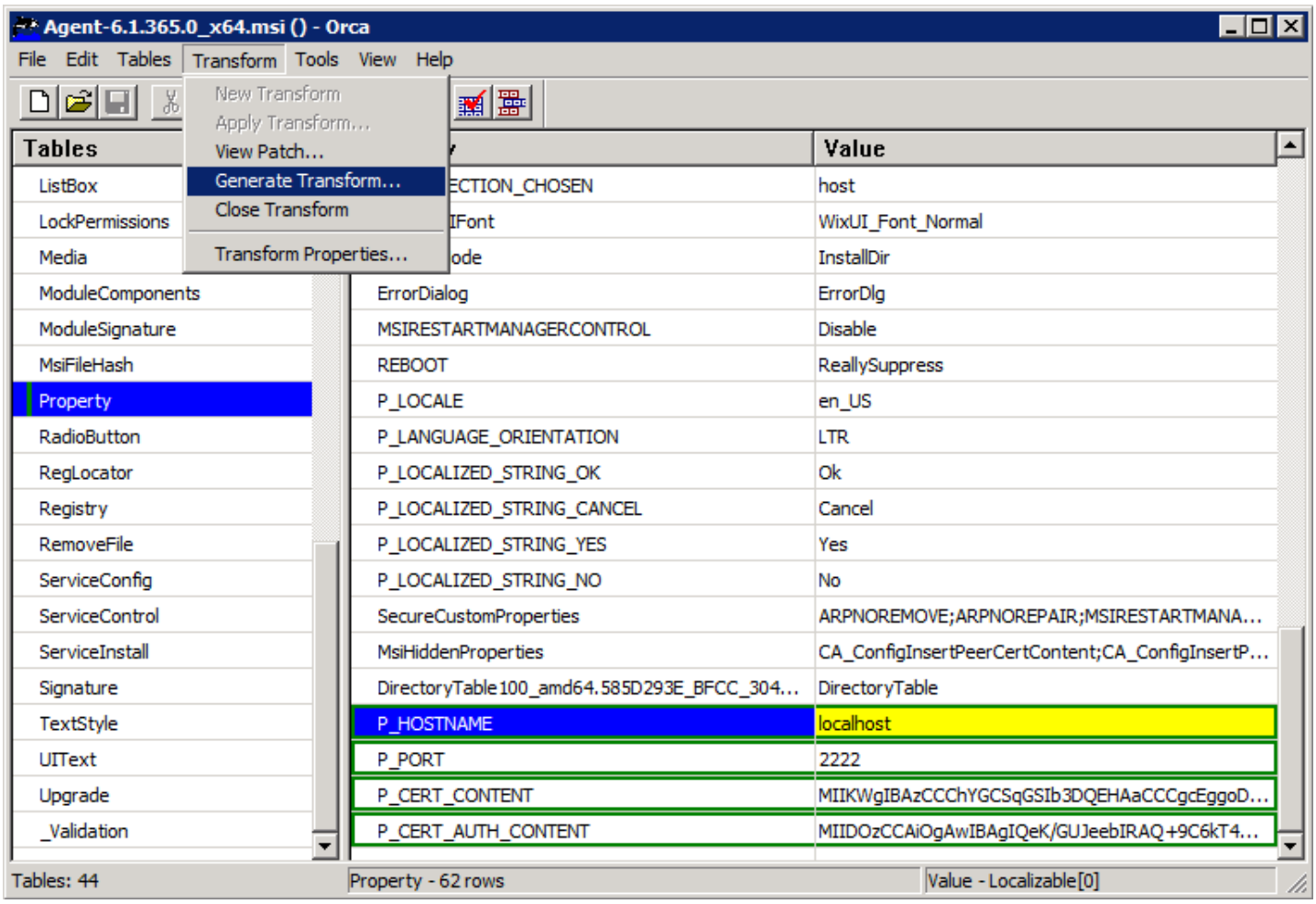
- In ERA Web Console, accedere ad **Amministrazione** > **Certificati** > **Certificato del peer**, fare clic su Certificato dell'agente e scegliere **Esporta come Base64**.
- Accedere ad **Amministrazione** > **Certificati** > **Autorità di certificazione**, fare clic su Autorità di certificazione ERA e scegliere **Esporta chiave pubblica come Base64**



- Aggiungere i contenuti del certificato e della chiave pubblica esportati nella tabella Proprietà in Orca utilizzando i seguenti nomi di proprietà:

Nome proprietà	Valore
P_CERT_CONTENT	<certificato del peer in formato Base64>
P_CERT_PASSWORD	<password del certificato del peer (non aggiungere questo valore se il campo Password è vuoto)>
P_CERT_AUTH_CONTENT	<chiave pubblica esportata dell'autorità di certificazione in formato Base64>

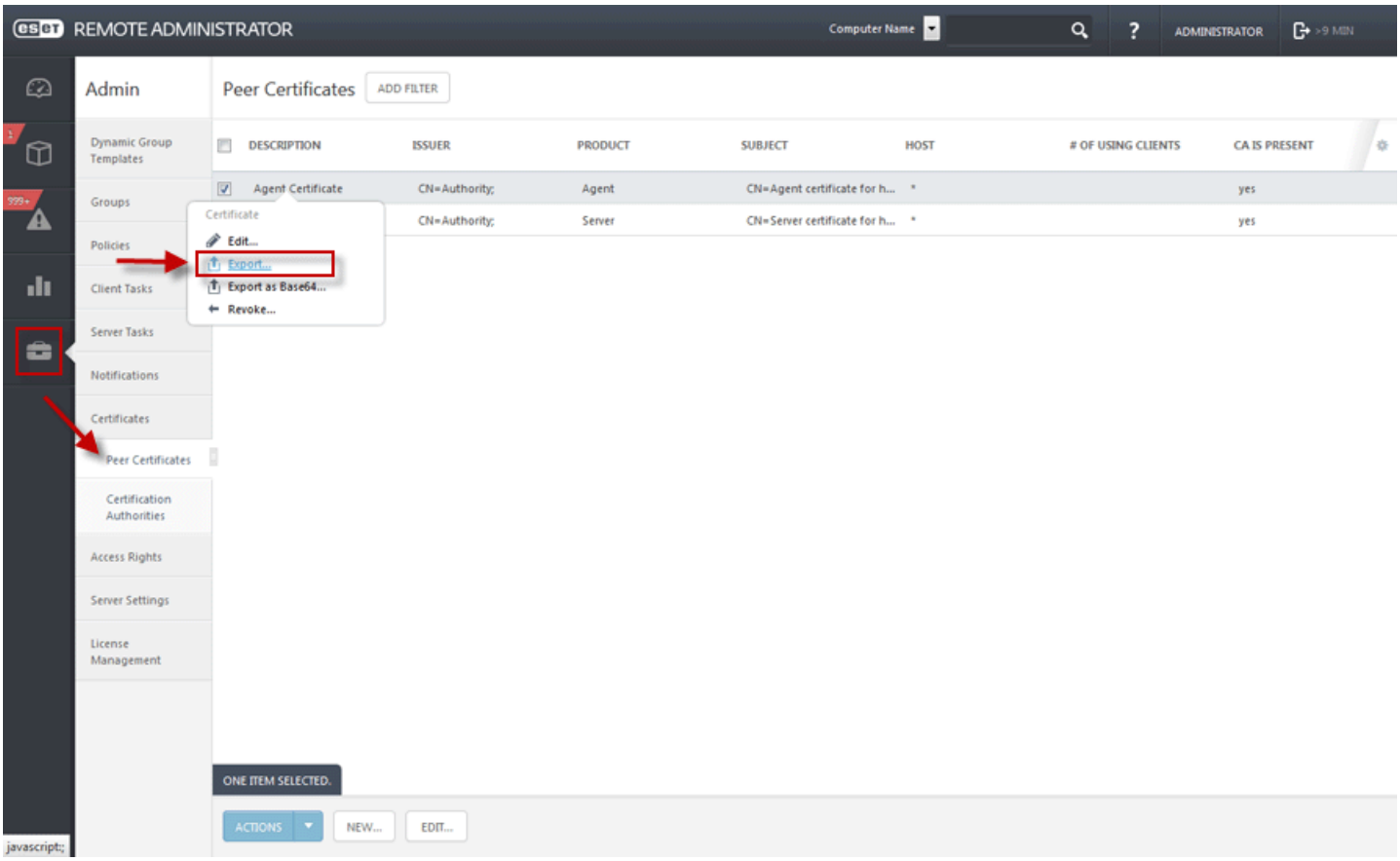
- Le nuove proprietà verranno evidenziate in verde. Fare clic su **Trasforma** e selezionare **Genera trasformazione...** per creare un file `.mst` .



2. È possibile scaricare i file del certificato e renderli accessibili dalla macchina di destinazione. Esportare il **Certificato del peer dell'agente** e il file della **Chiave pubblica** dall'**Autorità di certificazione** del server ERA e posizionarli in una cartella accessibile dalla macchina di destinazione su cui verrà installato l'agente ERA.

NOTA: questa opzione è **raccomandata** in casi specifici.

- Accedere ad **Amministrazione** > **Certificati** > **Certificato del peer**, fare clic su **Certificato dell'agente** e scegliere **Esporta...**
- Accedere ad **Amministrazione** > **Certificati** > **Autorità di certificazione**, fare clic su **Autorità di certificazione ERA** e scegliere **Esporta chiave pubblica**



- Utilizzare i file esportati e aggiungerne il percorso nella tabella Proprietà con Orca utilizzando i seguenti nomi di proprietà:

Nome proprietà	Valore
P_CERT_PATH	<percorso al certificato `.pfx` esportato>
P_CERT_PASSWORD	<password per il certificato `.pfx` (non aggiungere questo valore se il campo Password è vuoto)>
P_CERT_AUTH_PATH	<percorso alla chiave pubblica esportata dell'autorità di certificazione>

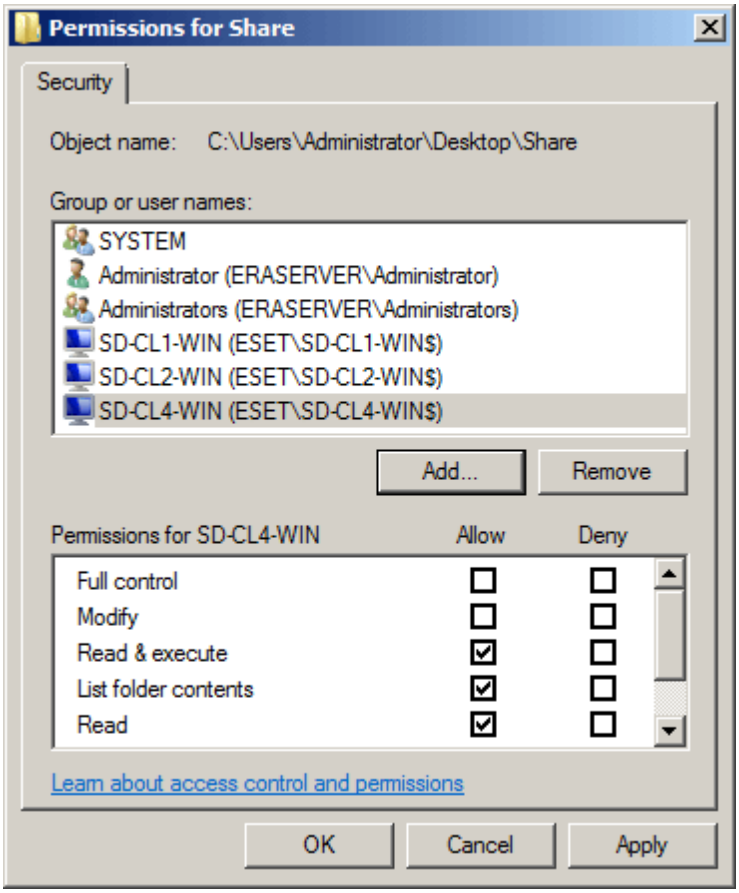
- Le proprietà aggiunte verranno evidenziate in verde. Fare clic su **Trasforma** e selezionare **Genera trasformazione...** per creare un file `.mst` .

4.4.3.2 Passaggi di distribuzione - GPO

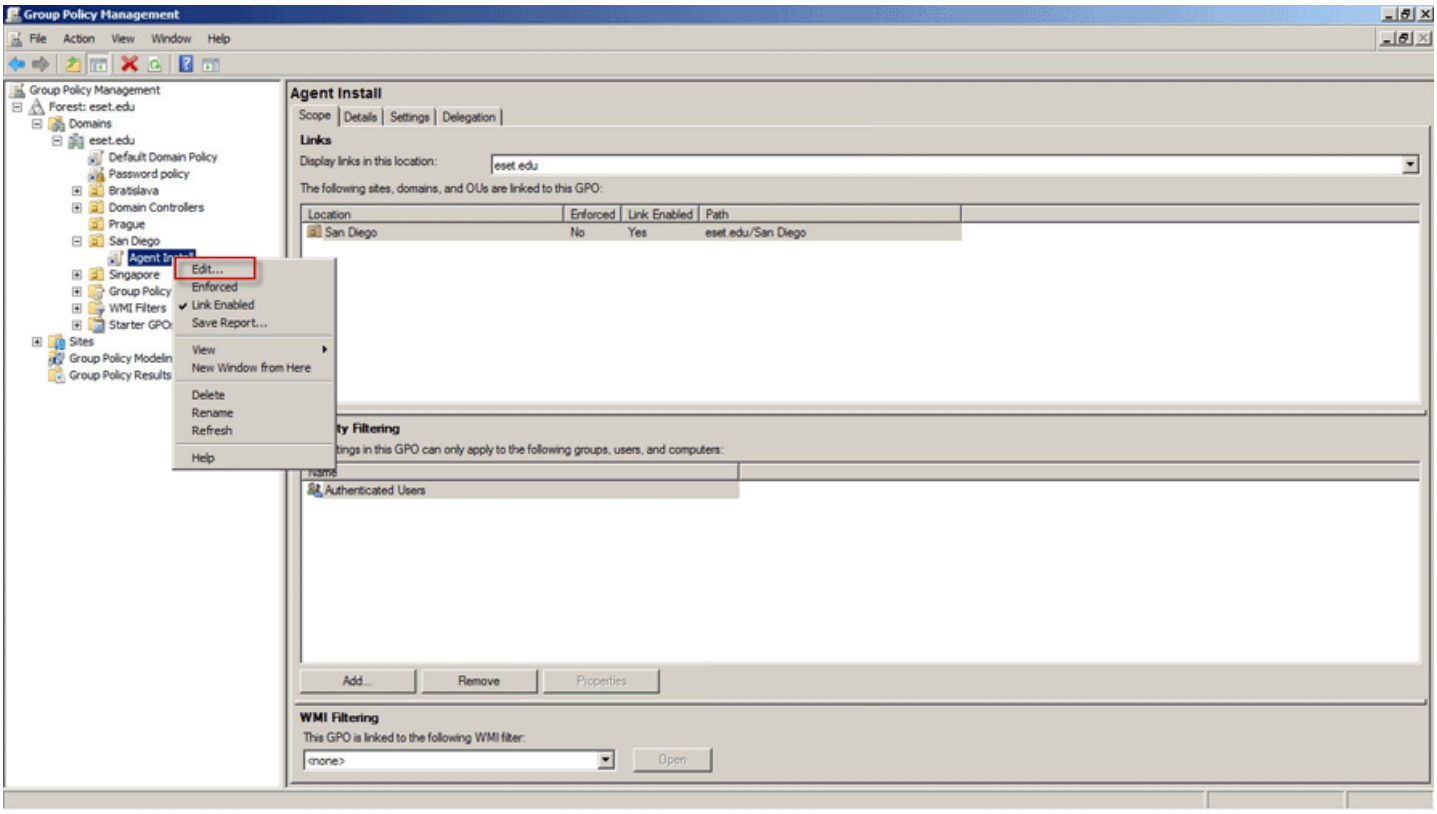
Seguire i passaggi sottostanti oppure consultare questo articolo della Knowledge Base per eseguire la distribuzione dell'agente ERA sui client mediante GPO:

1. Scaricare il file del programma di installazione dell'agente ERA `.msi` dalla pagina dei download di ESET.
2. Creare un file .mst di trasformazione del programma di installazione dell'agente ERA.
3. Posizionare il file del programma di installazione dell'agente ERA `.msi` e il file di trasformazione `.mst` in una cartella condivisa alla quale possono accedere i client di destinazione.

NOTA: i computer client richiederanno la lettura/l'esecuzione dell'accesso a questa cartella condivisa.

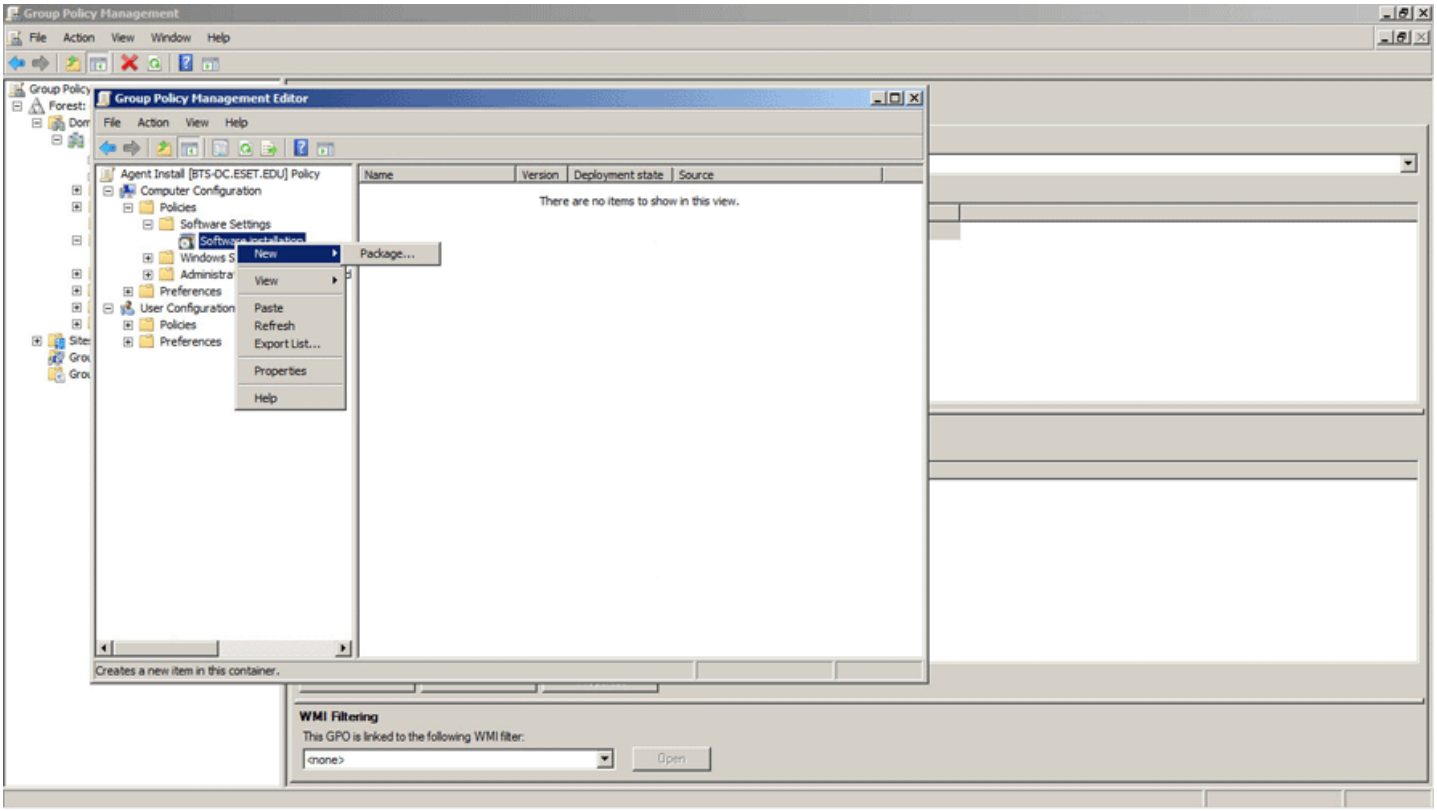


4. Utilizzare un oggetto del criterio del gruppo o crearne uno nuovo (fare clic con il pulsante destro del mouse su GPO e selezionare **Nuovo**). Nella struttura ad albero GPMC (console di gestione dei criteri dei gruppi), fare clic con il pulsante destro del mouse sul GPO che si desidera utilizzare e selezionare **Modifica**...



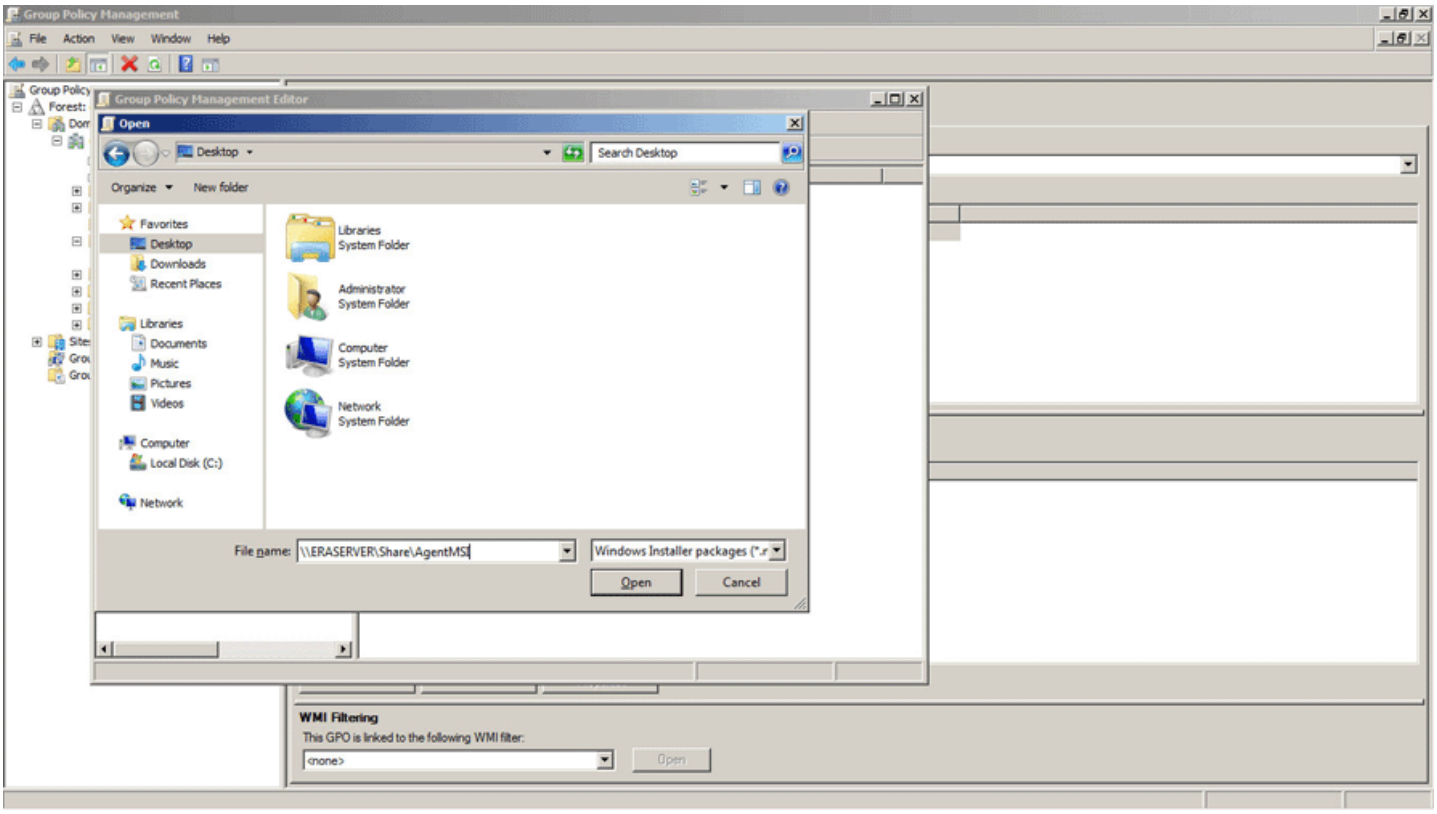
5. In Configurazione computer, accedere a **Criteri** > **Impostazioni software** > **Impostazioni software**.

6. Fare clic con il pulsante destro del mouse su **Installazione software**, selezionare **Nuova** e fare clic su **Pacchetto**... per creare una nuova configurazione per il pacchetto.

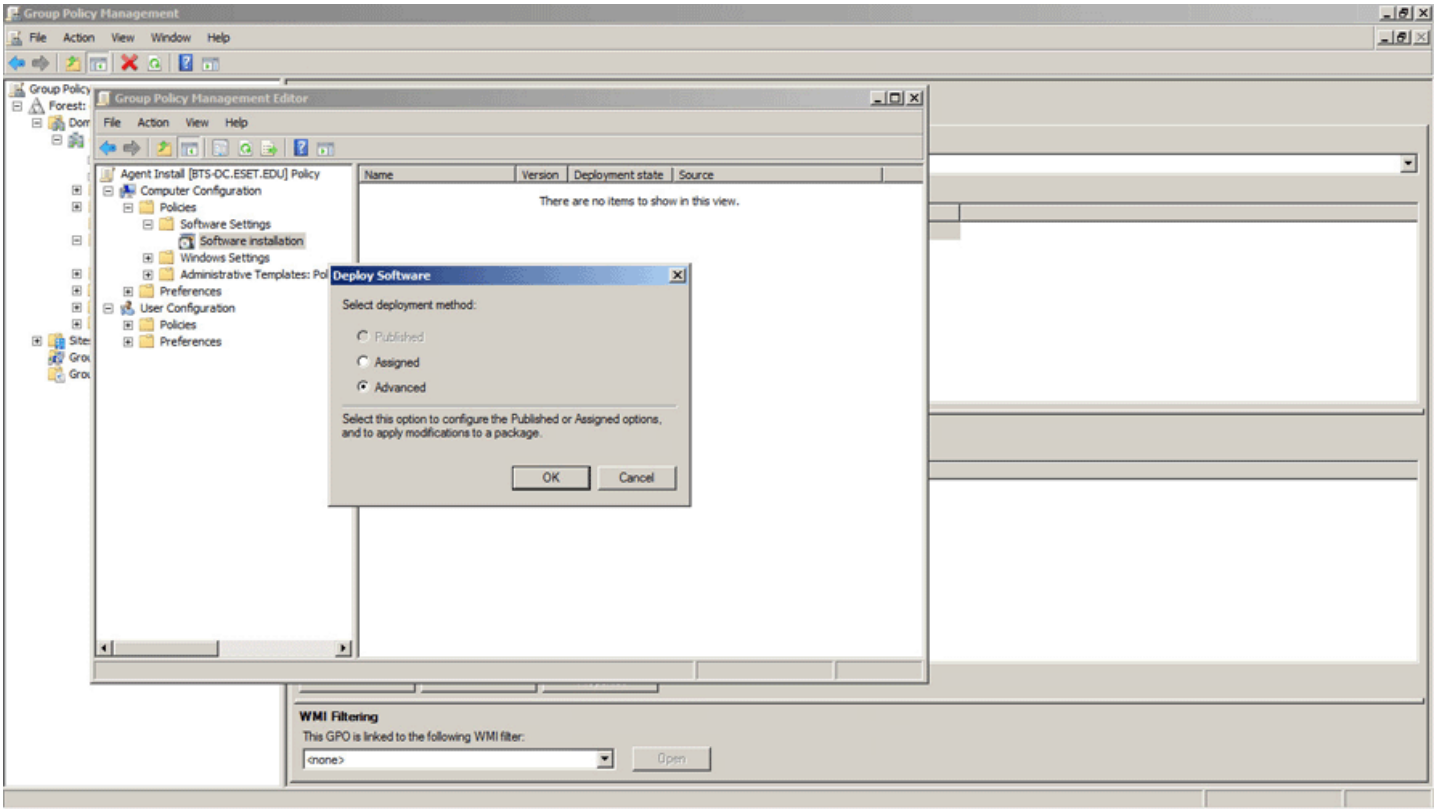


7. Accedere al punto in cui è posizionato il file dell'agente ERA `.msi` . Nella finestra di dialogo Apri, digitare il percorso completo della Universal Naming Convention (UNC) del pacchetto del programma di installazione condiviso che si desidera utilizzare. Ad esempio, `\\fileserver\share\filename.msi`

NOTA: assicurarsi di utilizzare il percorso UNC del pacchetto del programma di installazione condiviso.

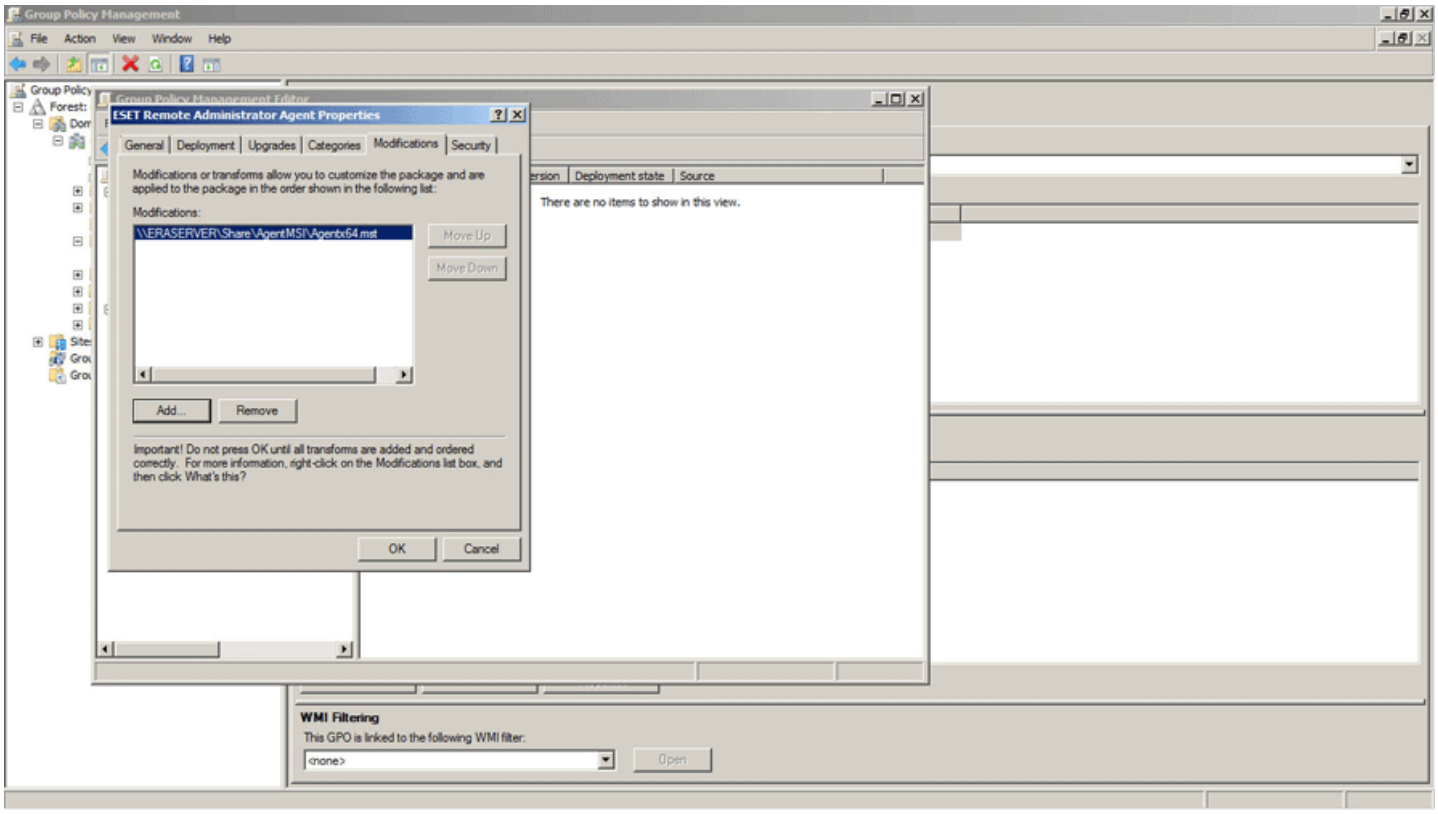


8. Fare clic su **Apri** e scegliere il metodo di distribuzione **Avanzato**.

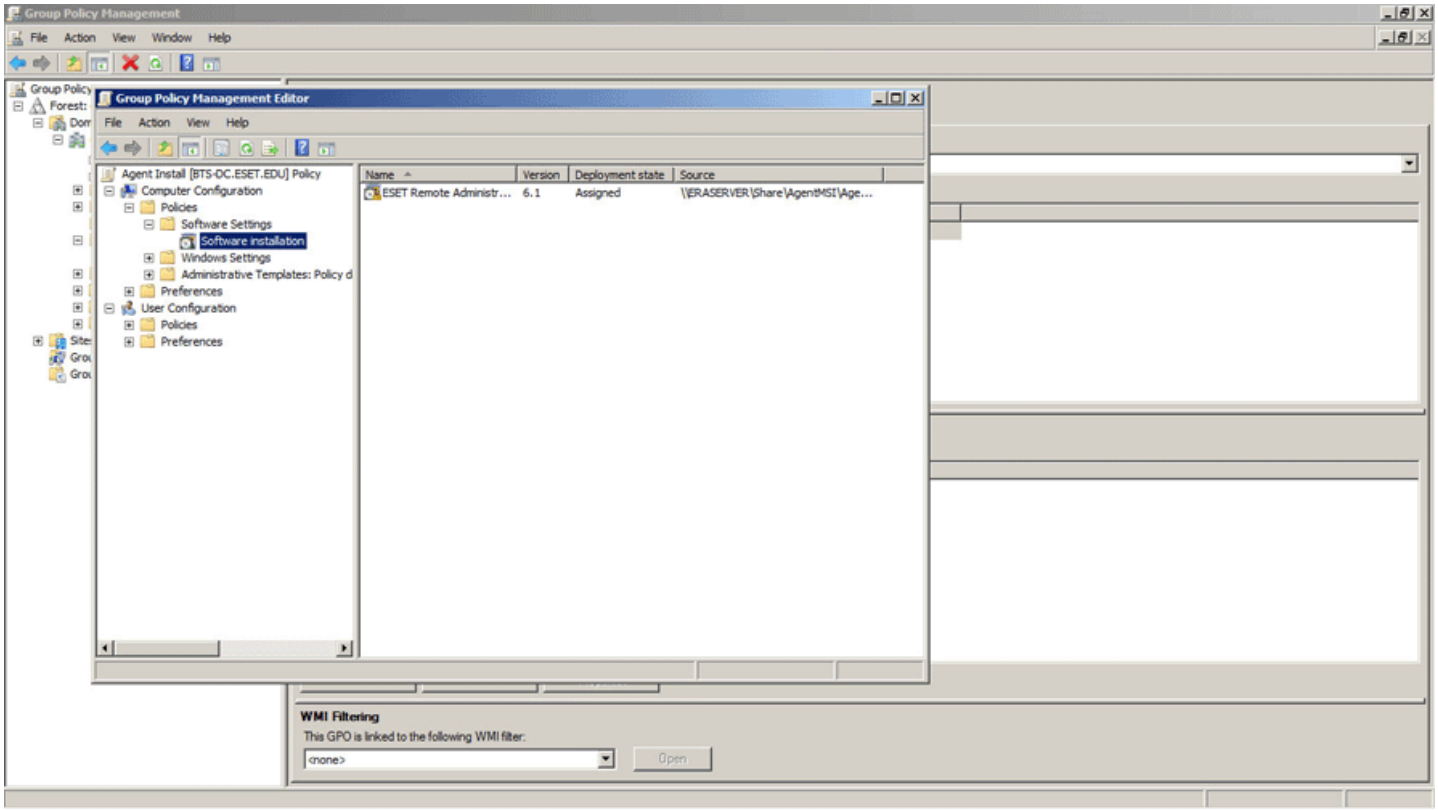


9. Tale operazione consentirà all'utente di configurare le opzioni di distribuzione. Selezionare la scheda **Modifiche** e ricercare il file di trasformazione del programma di installazione dell'agente ERA `.mst` .

NOTA: il percorso deve puntare alla stessa cartella condivisa di quella utilizzata al passaggio 7.


Group Policy Management
File Action View Window Help
ESET Remote Administrator Agent Properties
General Deployment Upgrades Categories Modifications Security
Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:
Modifications:
\\ERASERVER\Share\AgentMSI\Agentx64.mst
Move Up
Move Down
Add...
Remove
Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?
OK
Cancel
Deployment state
Source
There are no items to show in this view.
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open

10. Confermare la configurazione del pacchetto e procedere con la distribuzione GPO.

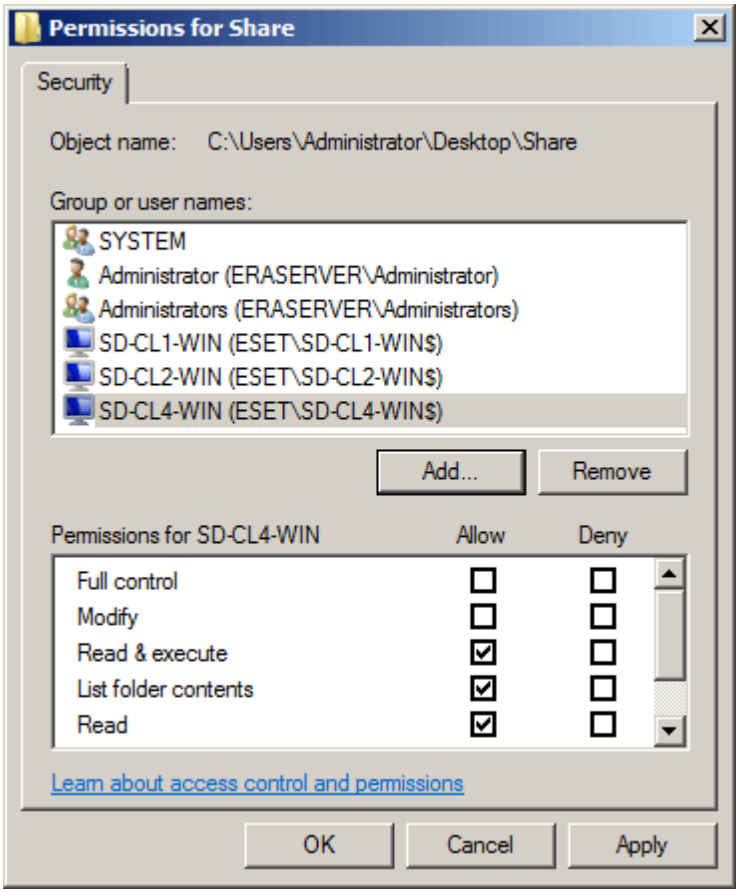


4.4.3.3 Passaggi di distribuzione - SCCM

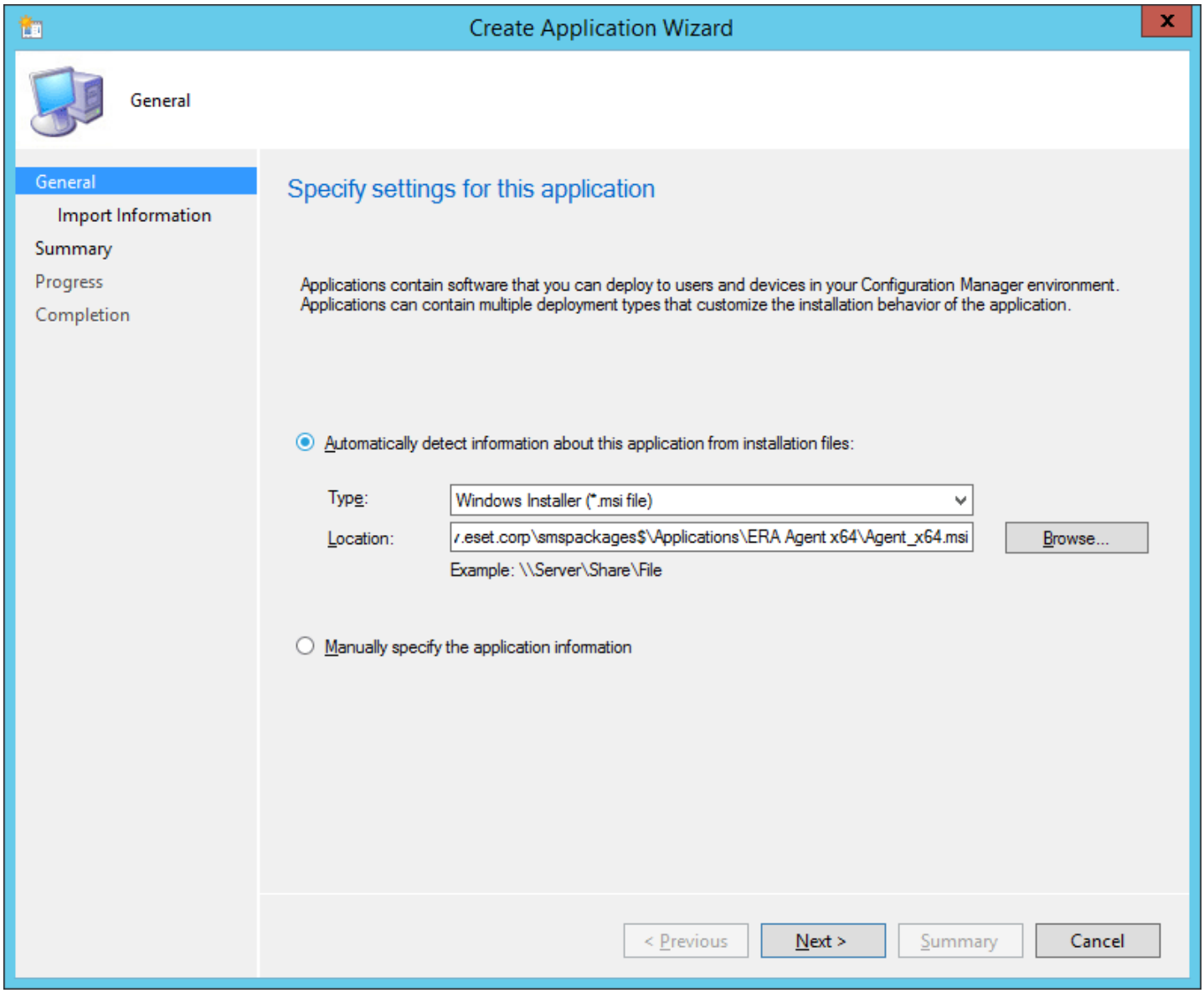
Seguire i passaggi sottostanti oppure consultare questo articolo della Knowledge Base per eseguire la distribuzione dell'agente ERA sui client mediante SCCM:

1. Scaricare il file del programma di installazione dell'agente ERA `.msi` dalla pagina dei download di ESET.
2. Creare un file .mst di trasformazione del programma di installazione dell'agente ERA.
3. Posizionare il file del programma di installazione dell'agente ERA `.msi` e il file di trasformazione `.mst` in una cartella condivisa.

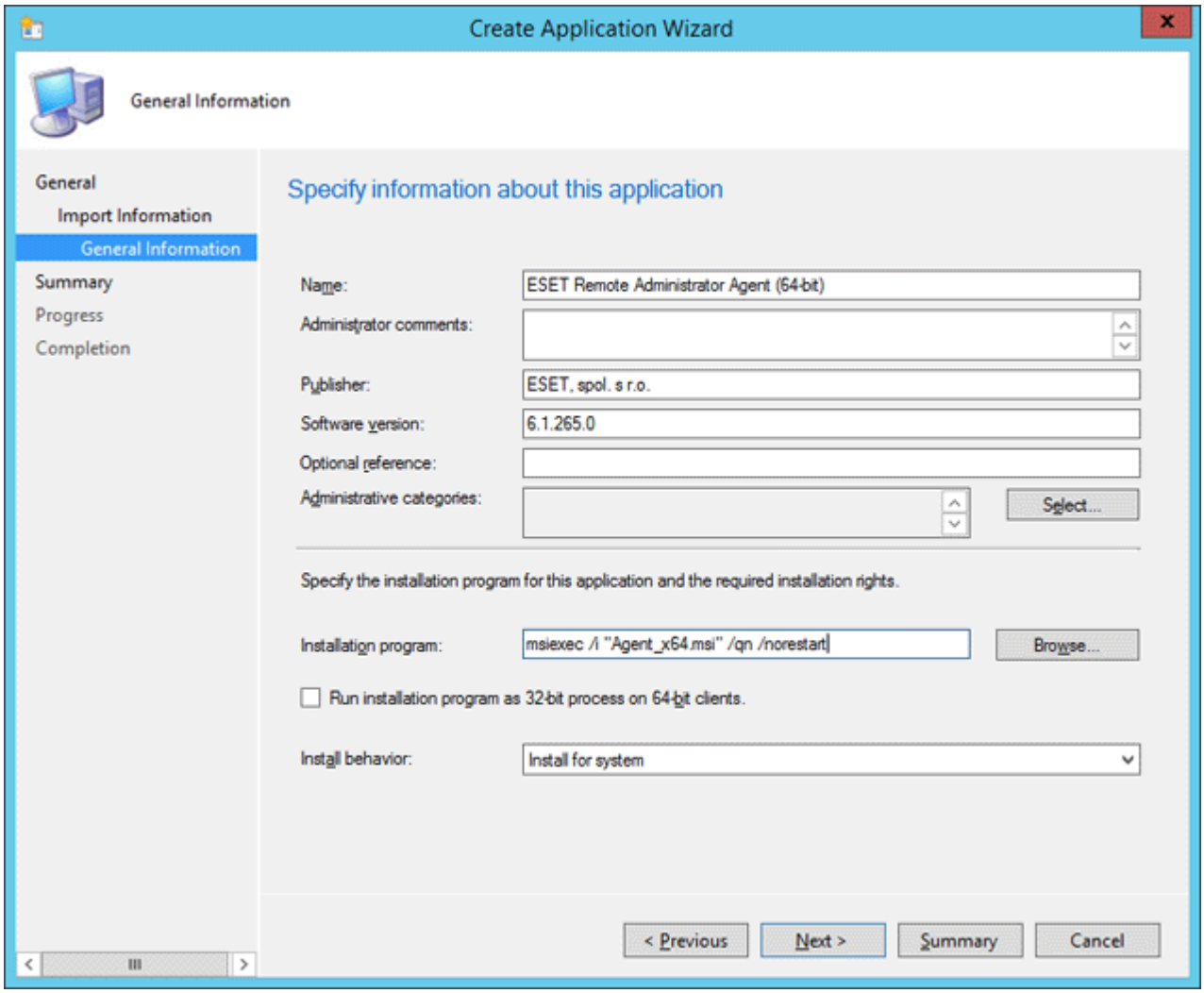
NOTA: i computer client richiederanno la lettura/l'esecuzione dell'accesso a questa cartella condivisa.



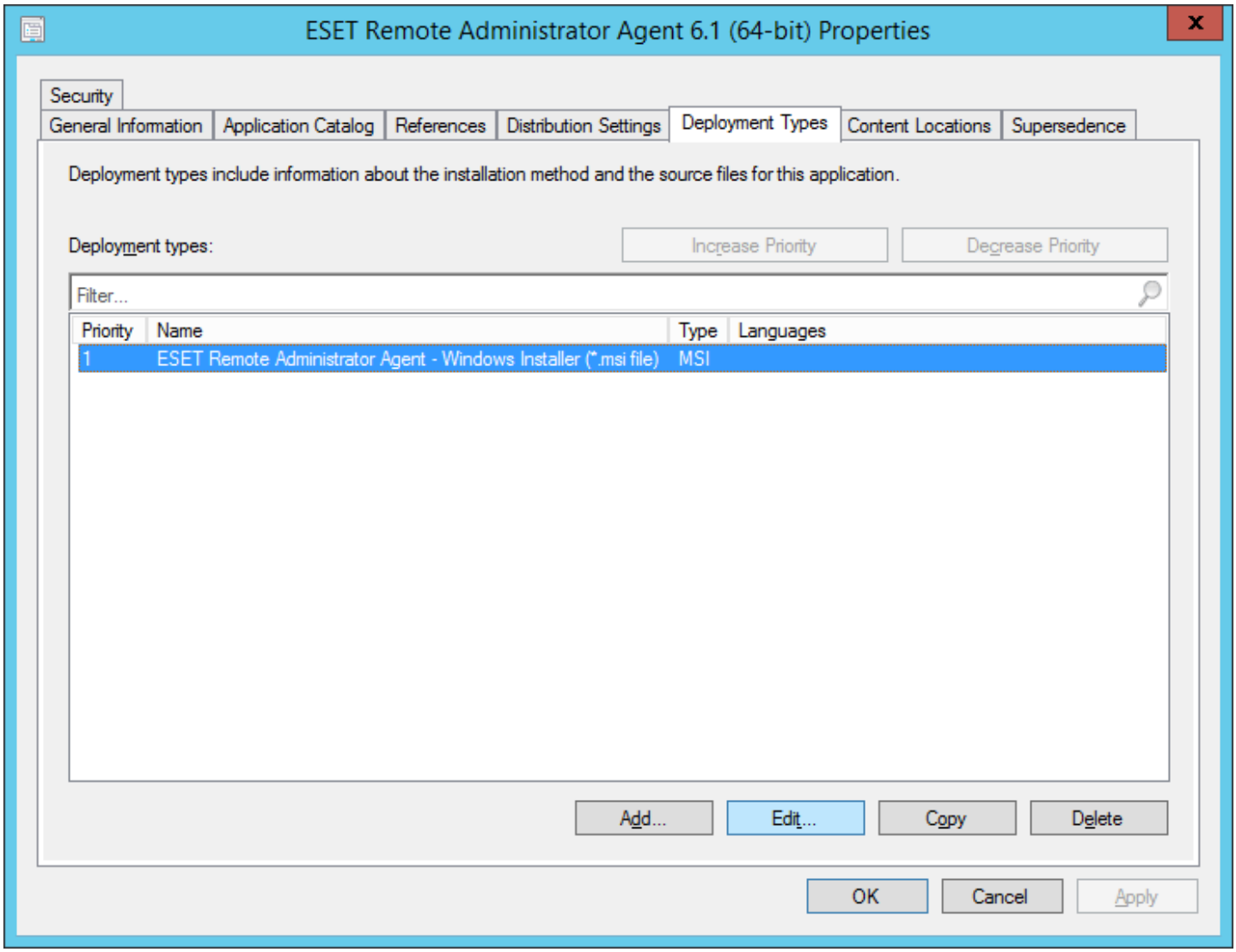
4. Aprire la console SCCM e fare clic su **Libreria software**. In **Gestione applicazioni**, fare clic con il pulsante destro del mouse su **Applicazioni** e scegliere **Crea applicazione**. Scegliere **Windows Installer (file *.msi)** e individuare la cartella di origine in cui è stato salvato il file del programma di installazione dell'agente ERA `.msi` .



5. Specificare tutte le informazioni richieste sull'applicazione e fare clic su **Avanti**.

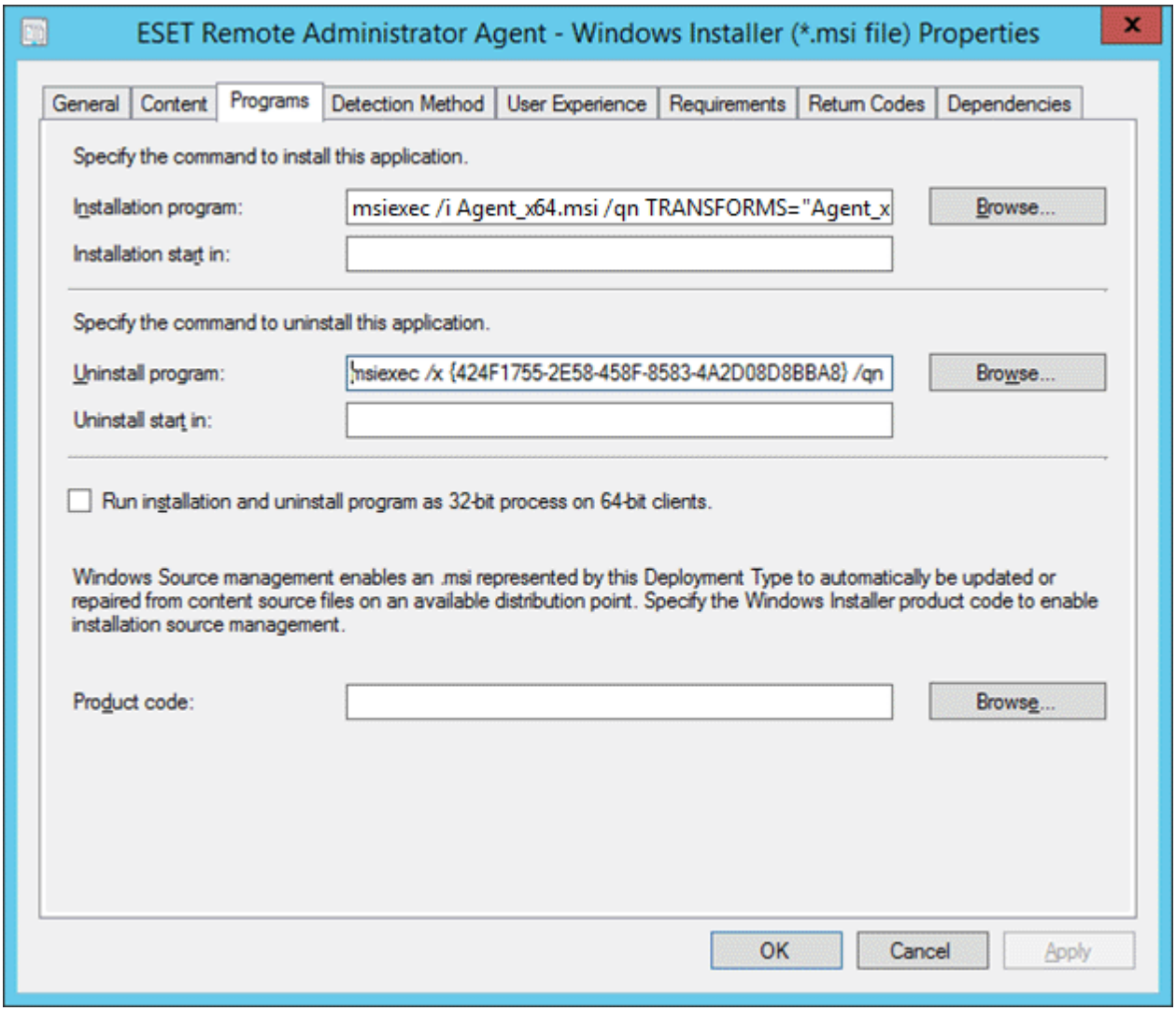


6. Fare clic con il pulsante destro del mouse su ESET Remote Administrator Agent Application, fare clic sulla scheda **Tipi di distribuzione**, selezionare l'unica distribuzione presente e fare clic su **Modifica**.

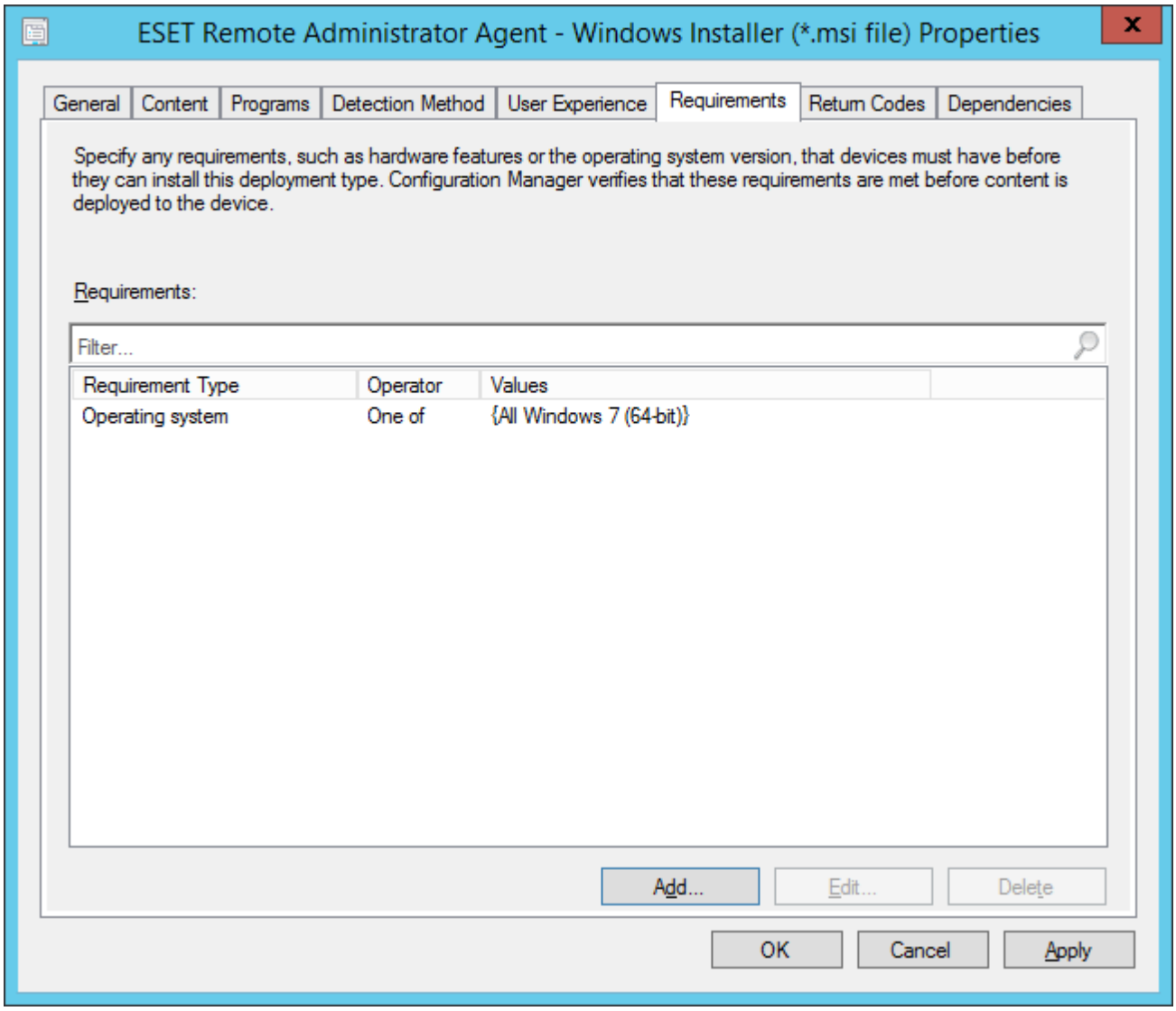


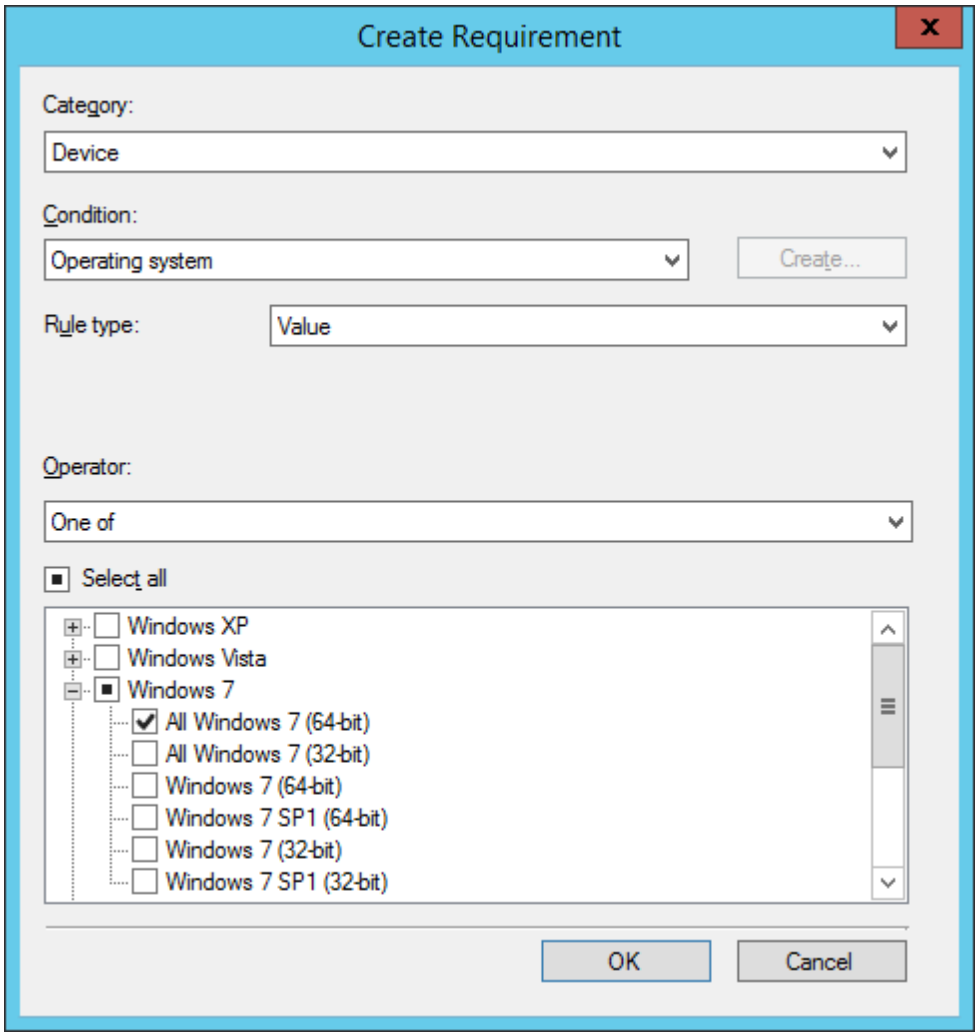
7. Fare clic sulla scheda Programmi e modificare il campo Programma di installazione in modo che contenga la seguente stringa msiexec/iAgent_x64.msi/qn TRANSFORMS="Agent_x64.mst (in caso di utilizzo di pacchetti a 32 bit, questa stringa sarà leggermente diversa in quanto conterrà "x32" al posto di "x64").

8. Modificare il campo Disinstalla programma in modo che contenga la stringa msiexec/x {424F1755-2E58-458F-8583-4A2D08D8BBA8} /qn/norestart.

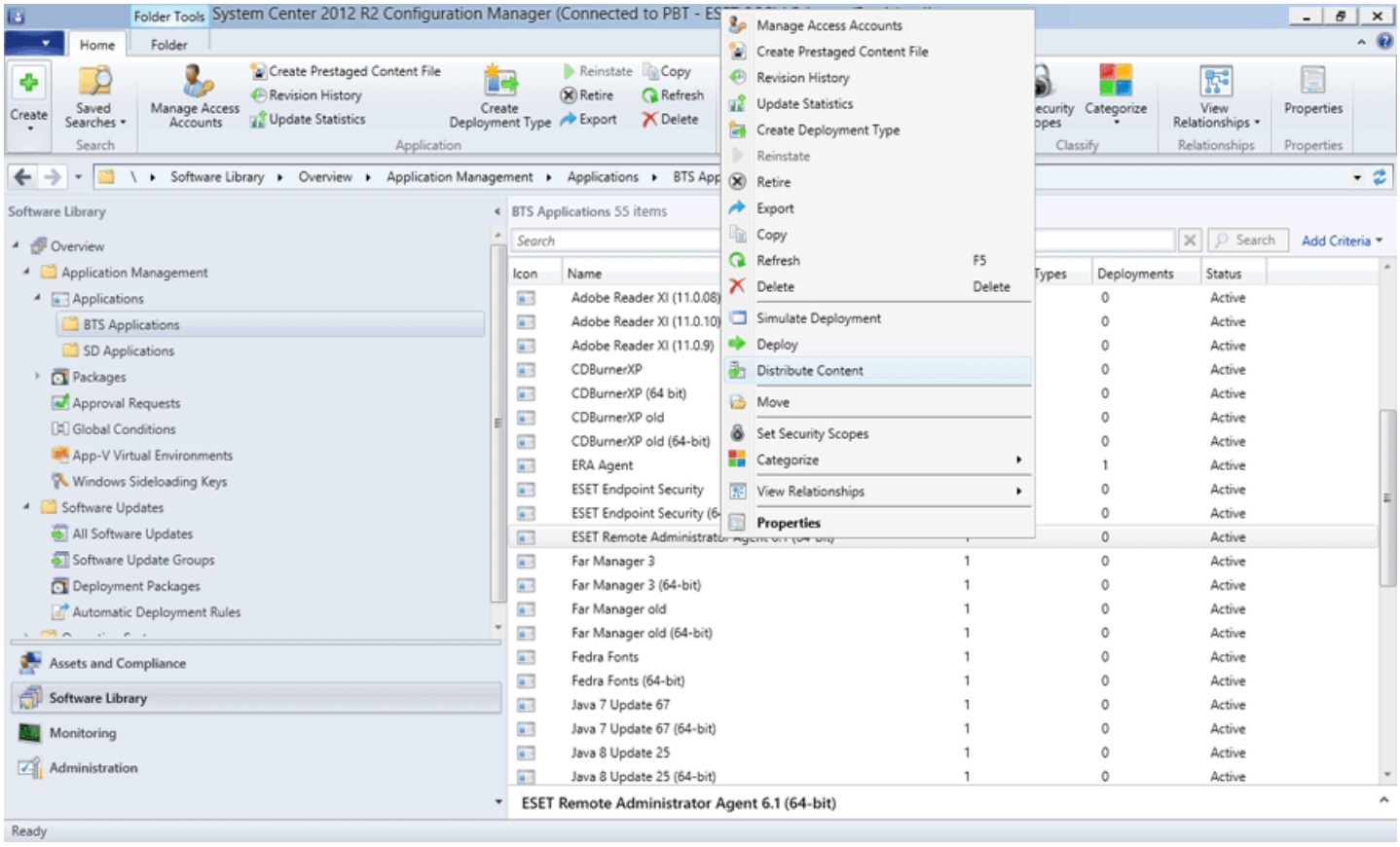

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify the command to install this application.
Installation program:
msiexec /i Agent_x64.msi /qn TRANSFORMS="Agent_x
Browse...
Installation start in:
Specify the command to uninstall this application.
Uninstall program:
msiexec /x {424F1755-2E58-458F-8583-4A2D08D8BBA8} /qn
Browse...
Uninstall start in:
Run installation and uninstall program as 32-bit process on 64-bit clients.
Windows Source management enables an .msi represented by this Deployment Type to automatically be updated or repaired from content source files on an available distribution point. Specify the Windows Installer product code to enable installation source management.
Product code:
Browse...
OK
Cancel
Apply

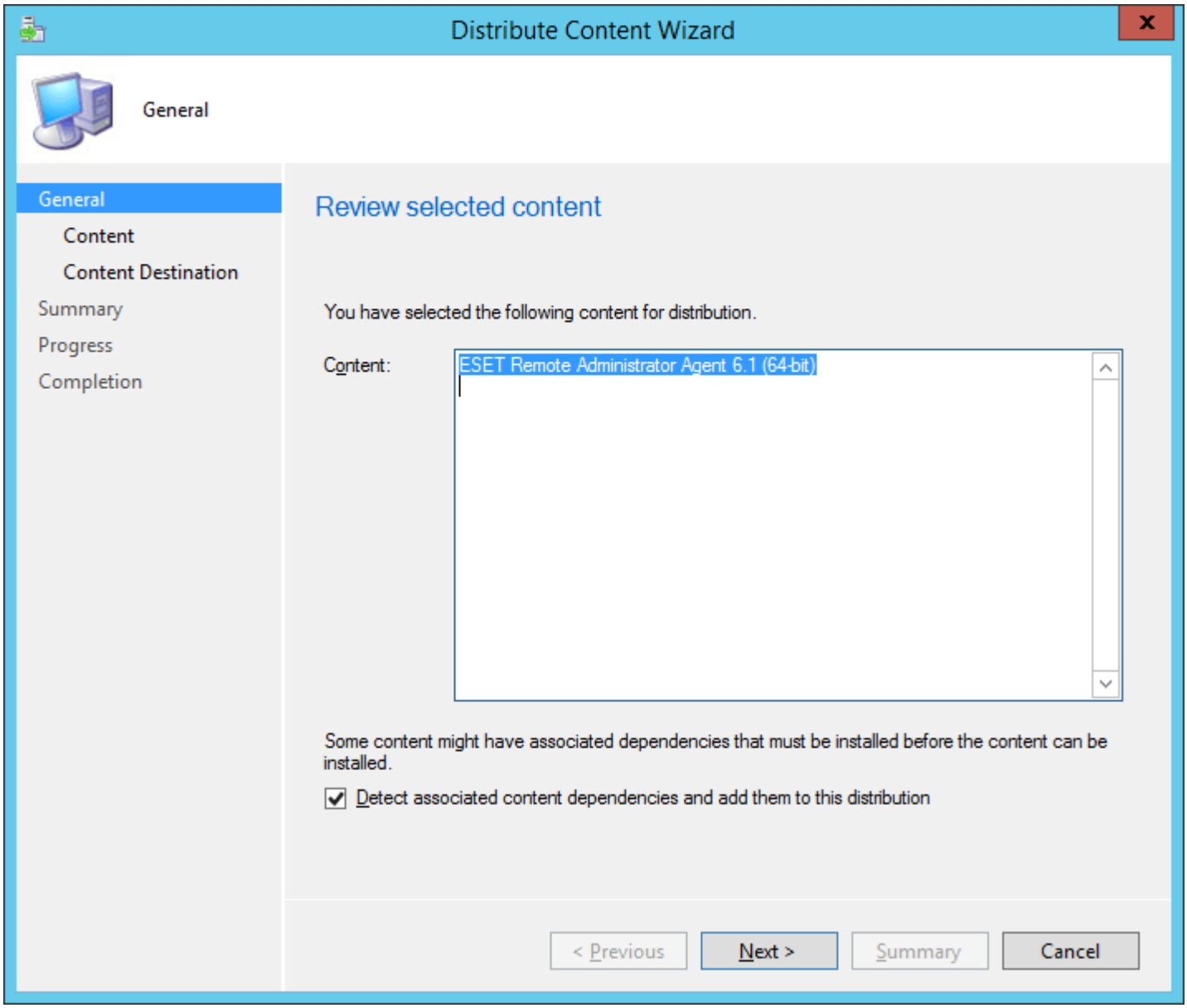
9. Fare clic sulla scheda **Requisiti**, quindi su Aggiungi. Selezionare il sistema operativo dal menu a discesa Condizione, selezionare Uno di dal menu a discesa Operatore e specificare i sistemi operativi su cui verranno installati selezionando le caselle di controllo appropriate. Al termine dell'operazione, fare clic su OK, quindi nuovamente su OK per chiudere eventuali finestre aperte e salvare le modifiche.

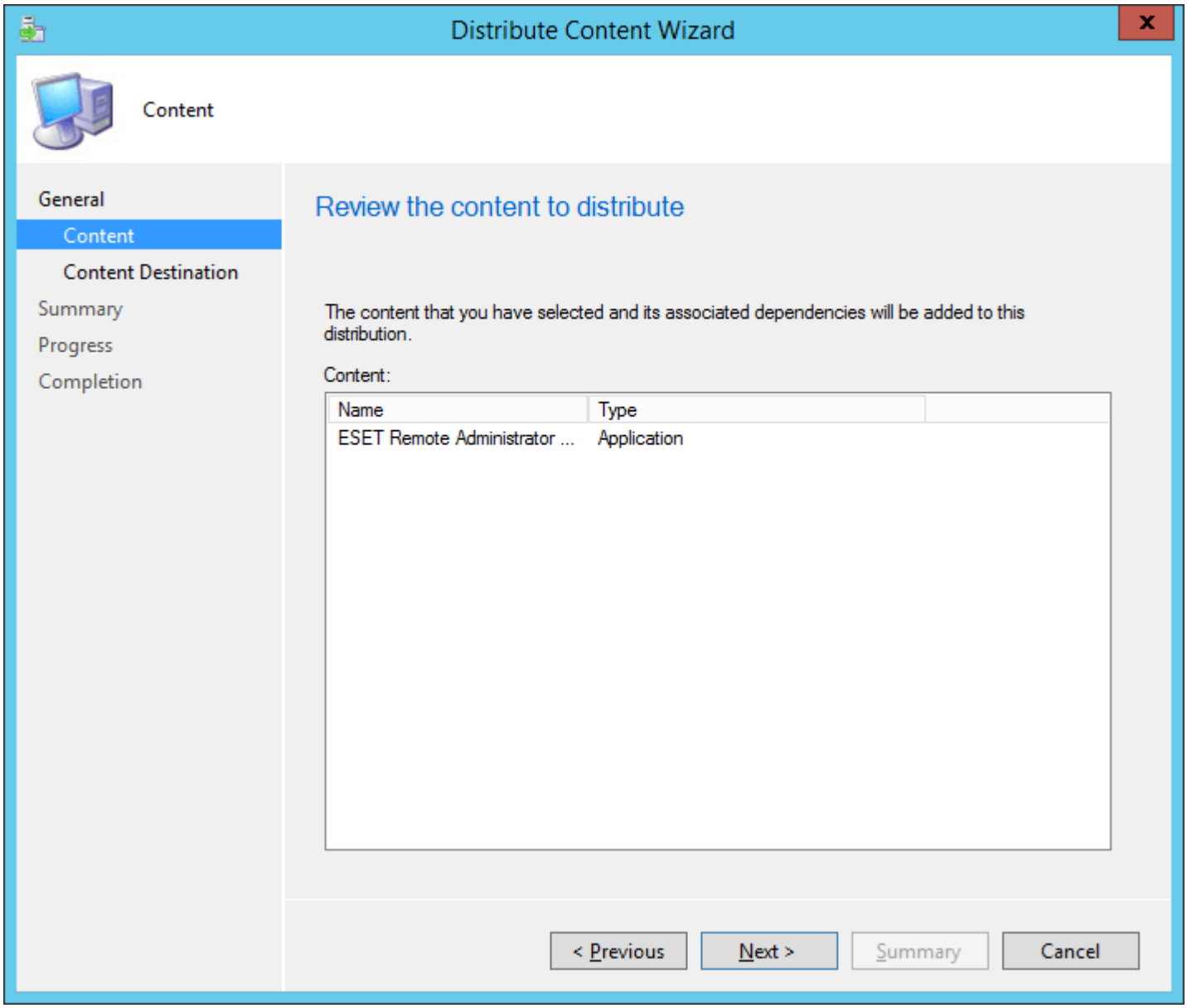

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply



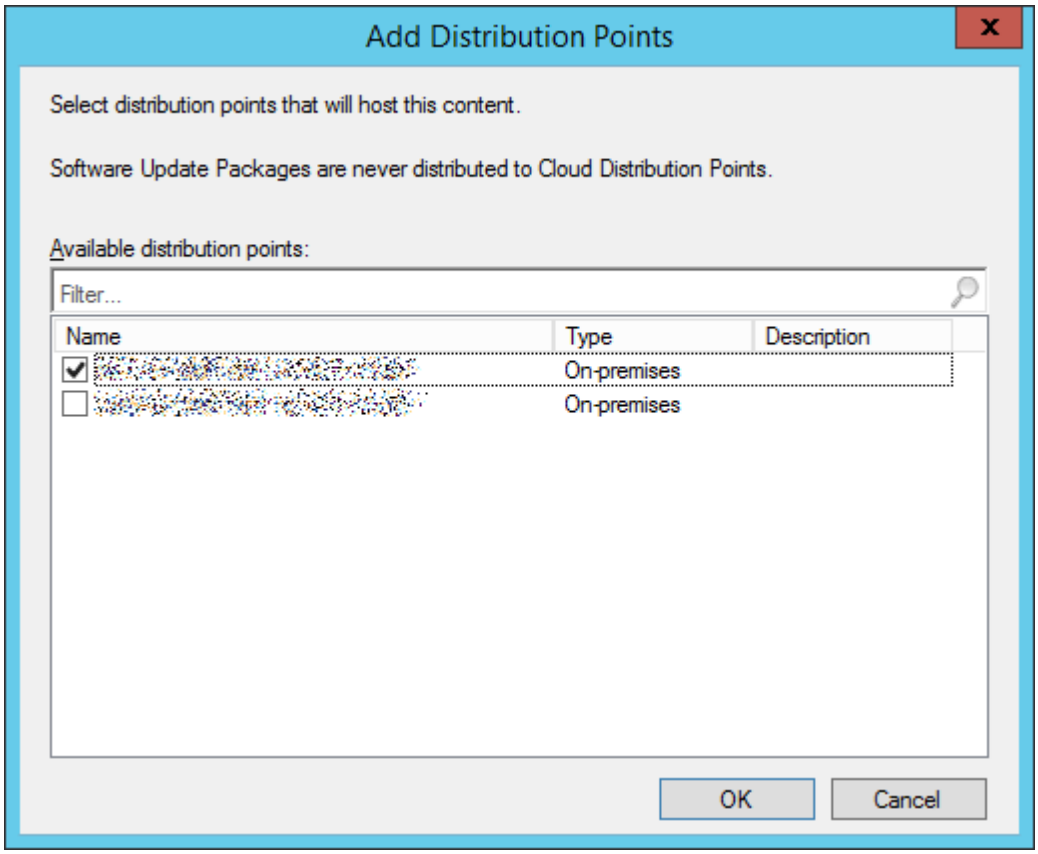
10. Nella libreria software di System Center, fare clic con il pulsante destro del mouse sulla nuova applicazione e selezionare Distribuisci contenuto dal menu contestuale. Seguire i prompt nella procedura guidata di distribuzione del software per completare la distribuzione dell'applicazione.

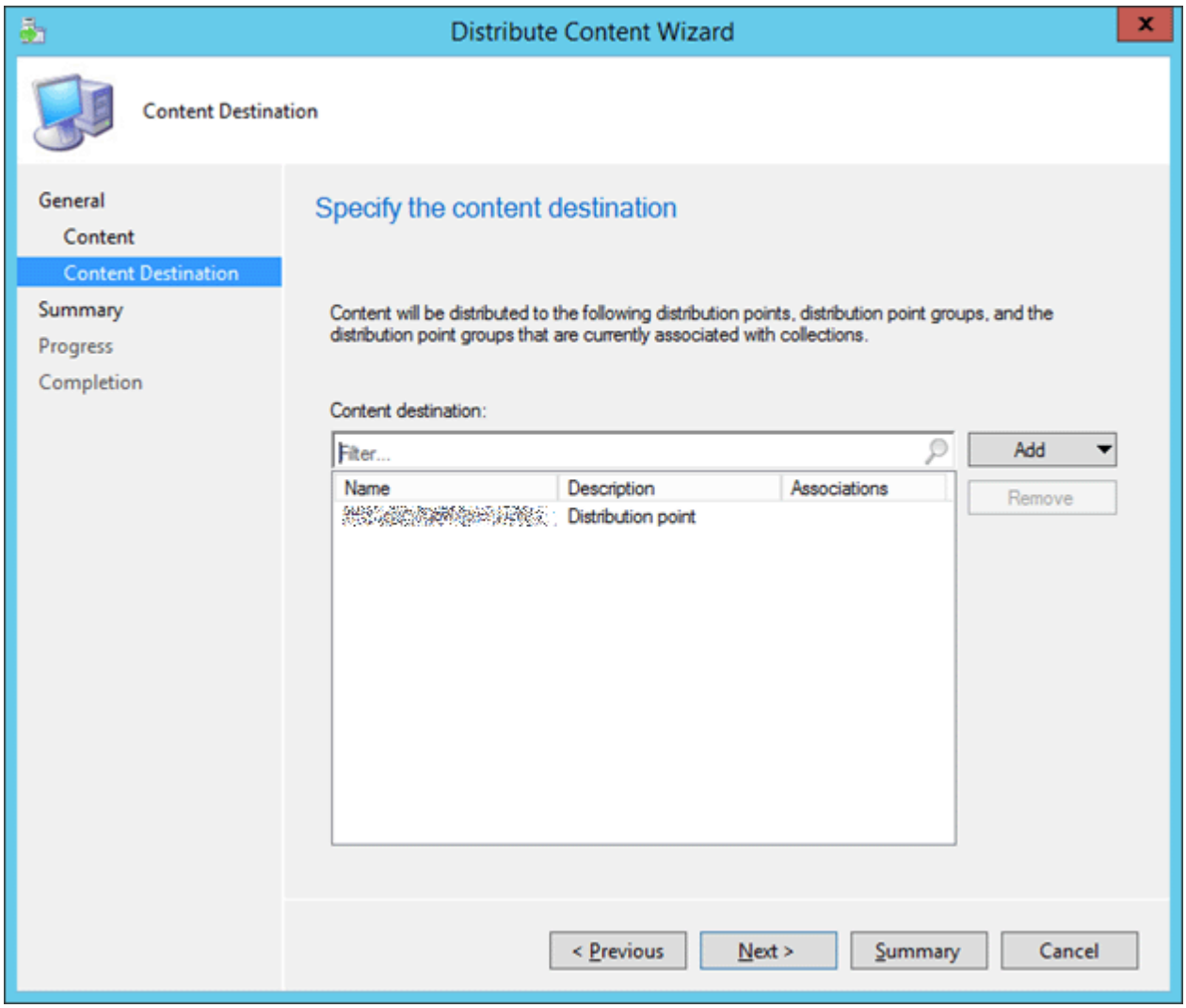


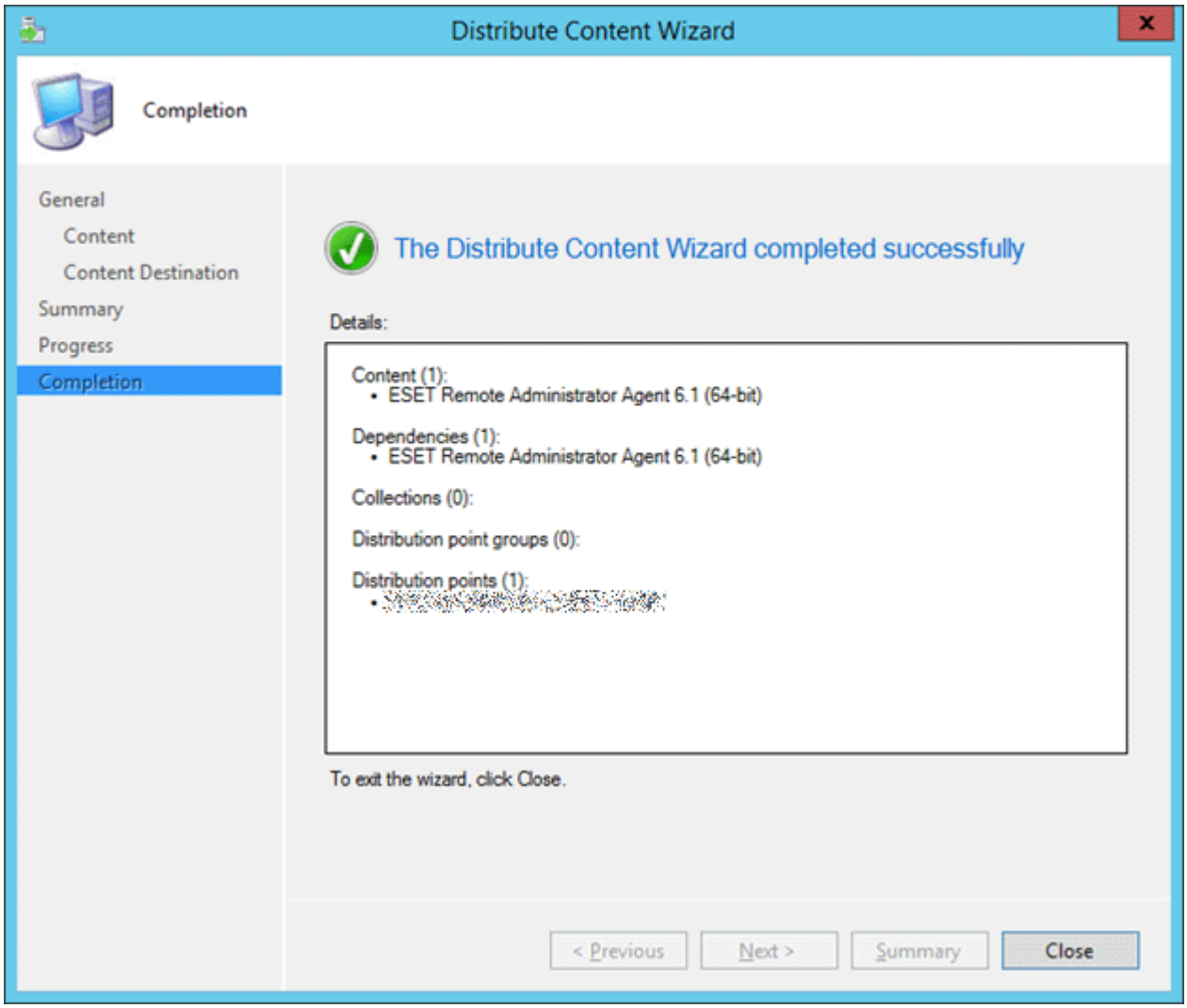

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent 6.1 (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

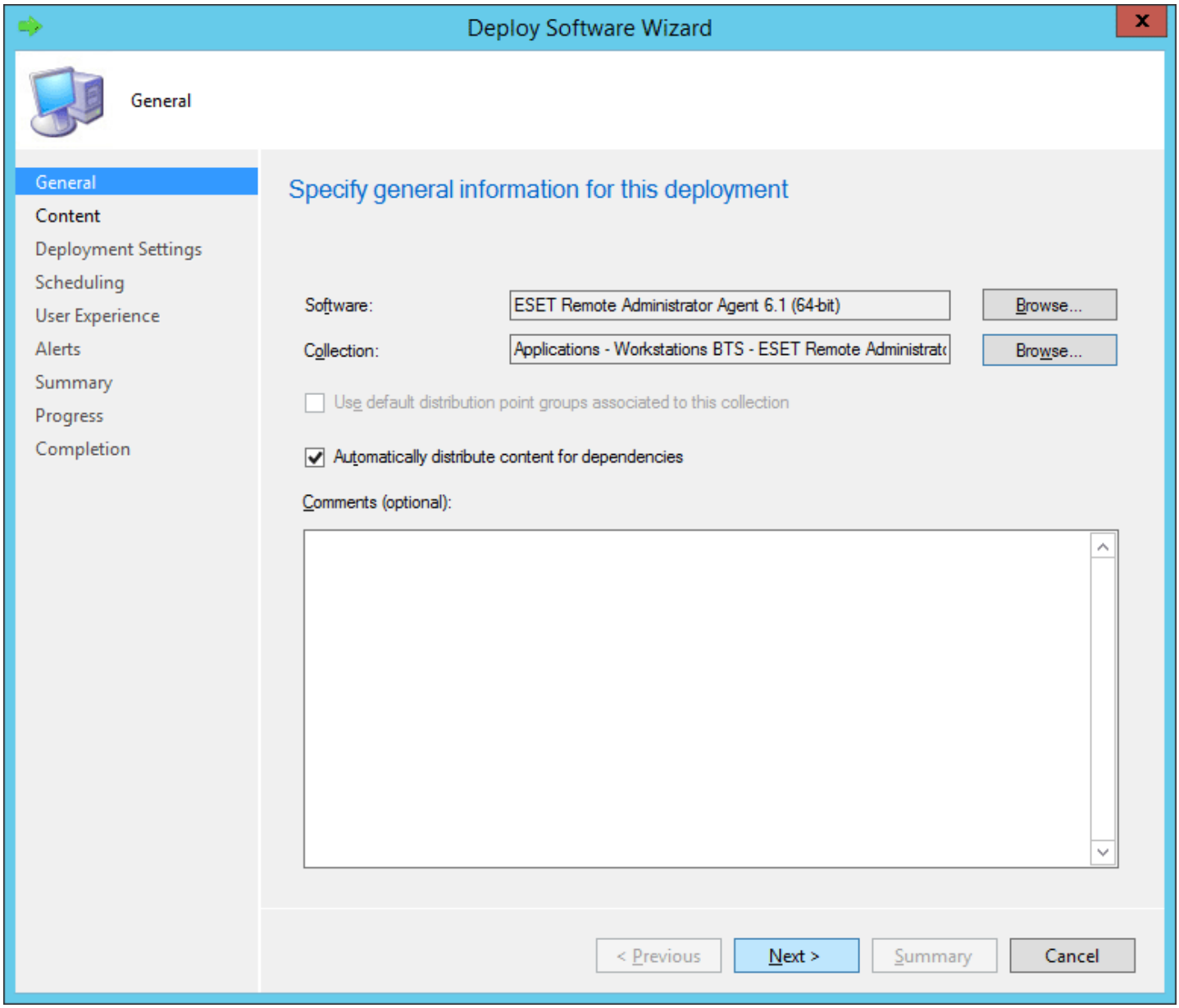


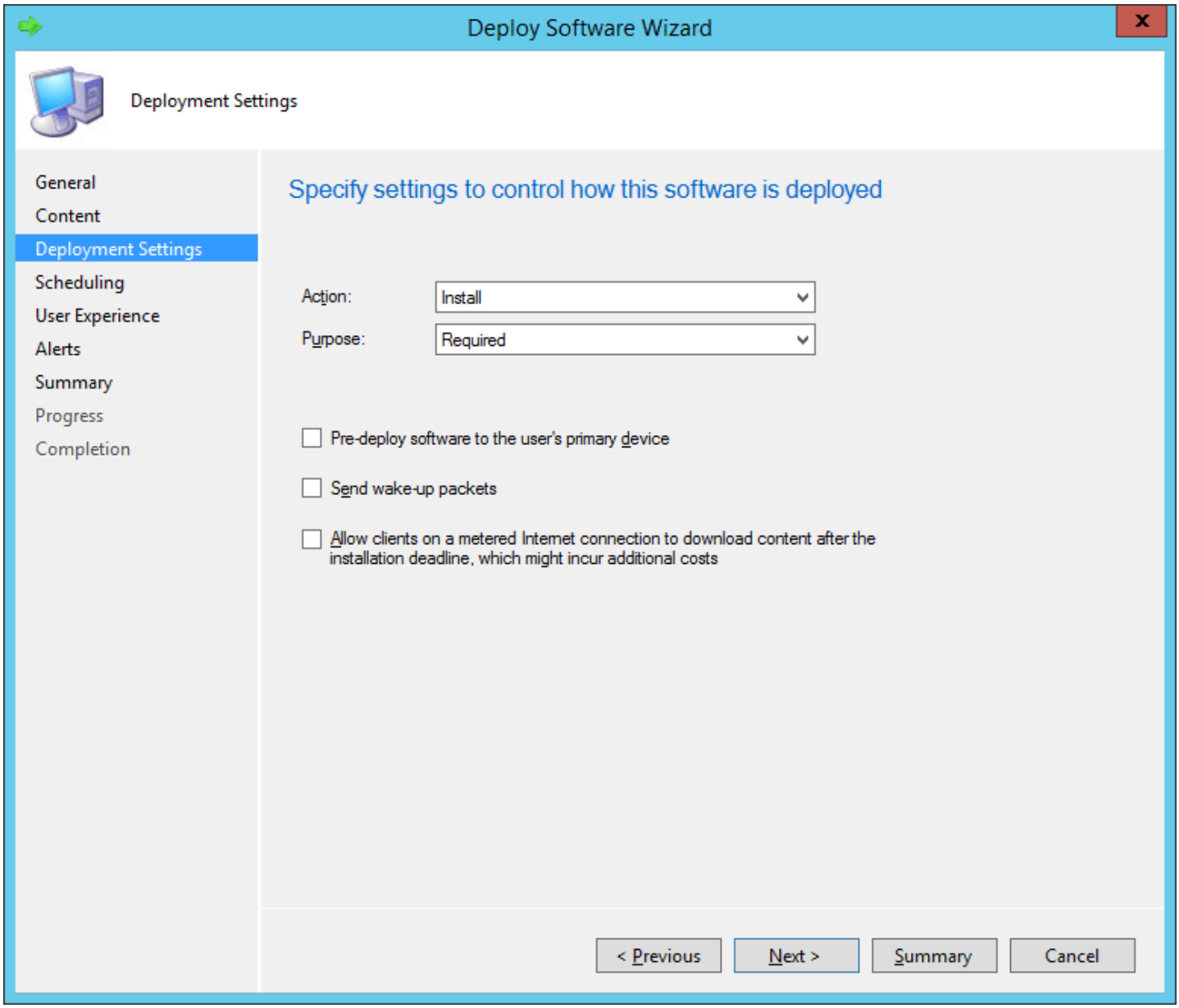
11. Fare clic con il pulsante destro del mouse sull'applicazione e scegliere **Distribuisci**. Seguire la procedura guidata e scegliere il punto di raccolta e di destinazione in cui si desidera effettuare la distribuzione dell'agente.

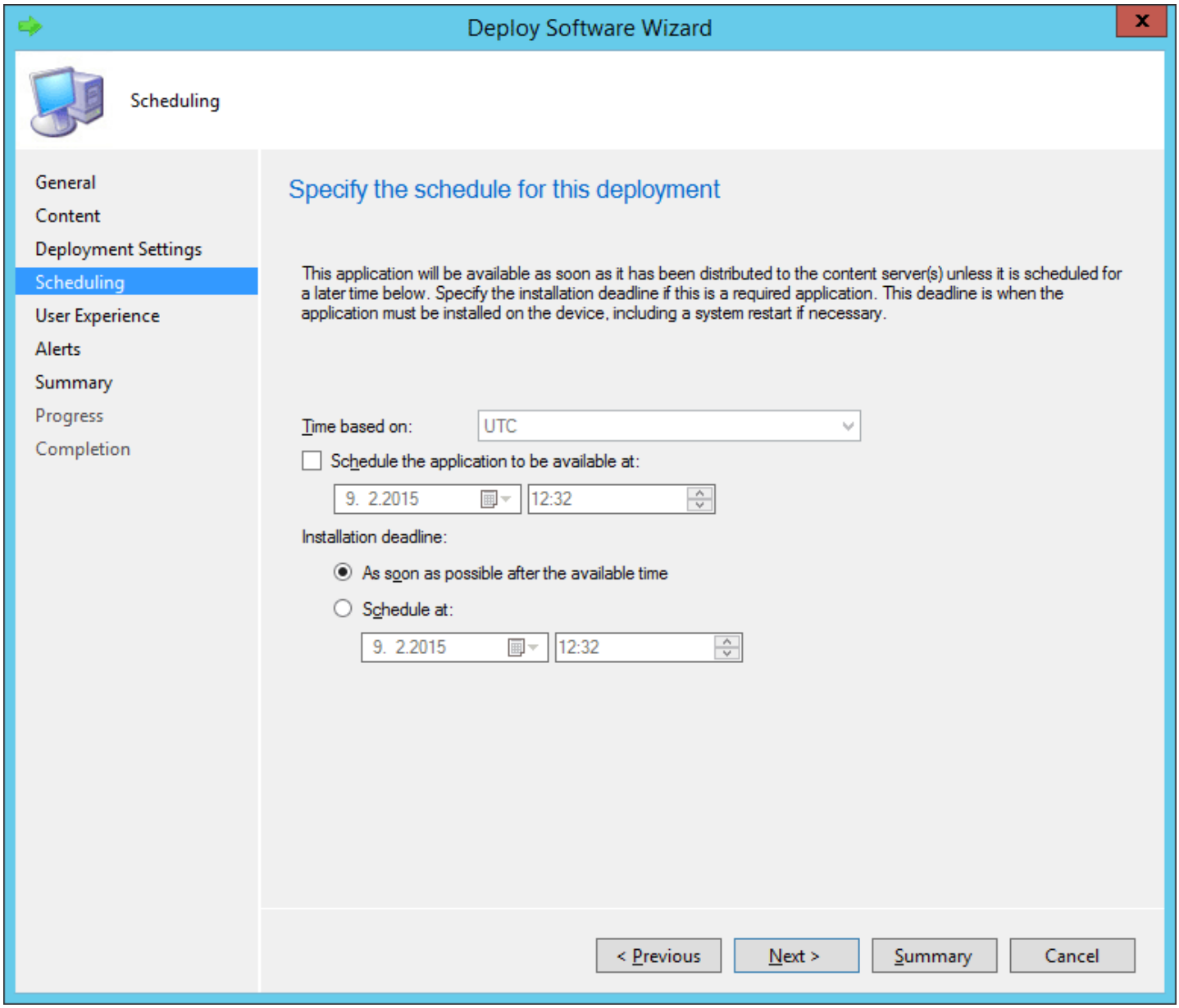

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

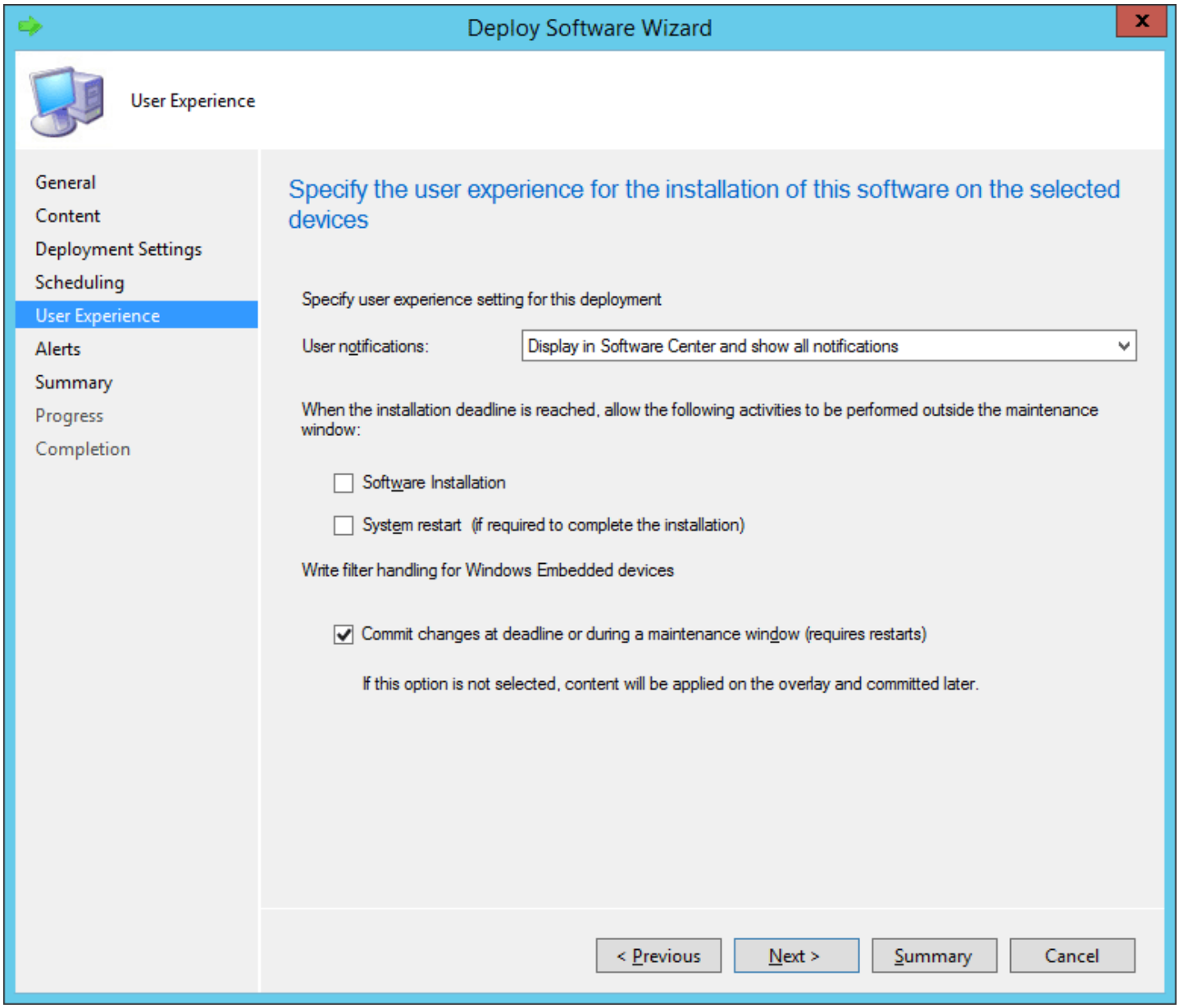

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Filter...
Add
Remove
Name
Description
Associations
Distribution point
< Previous
Next >
Summary
Cancel

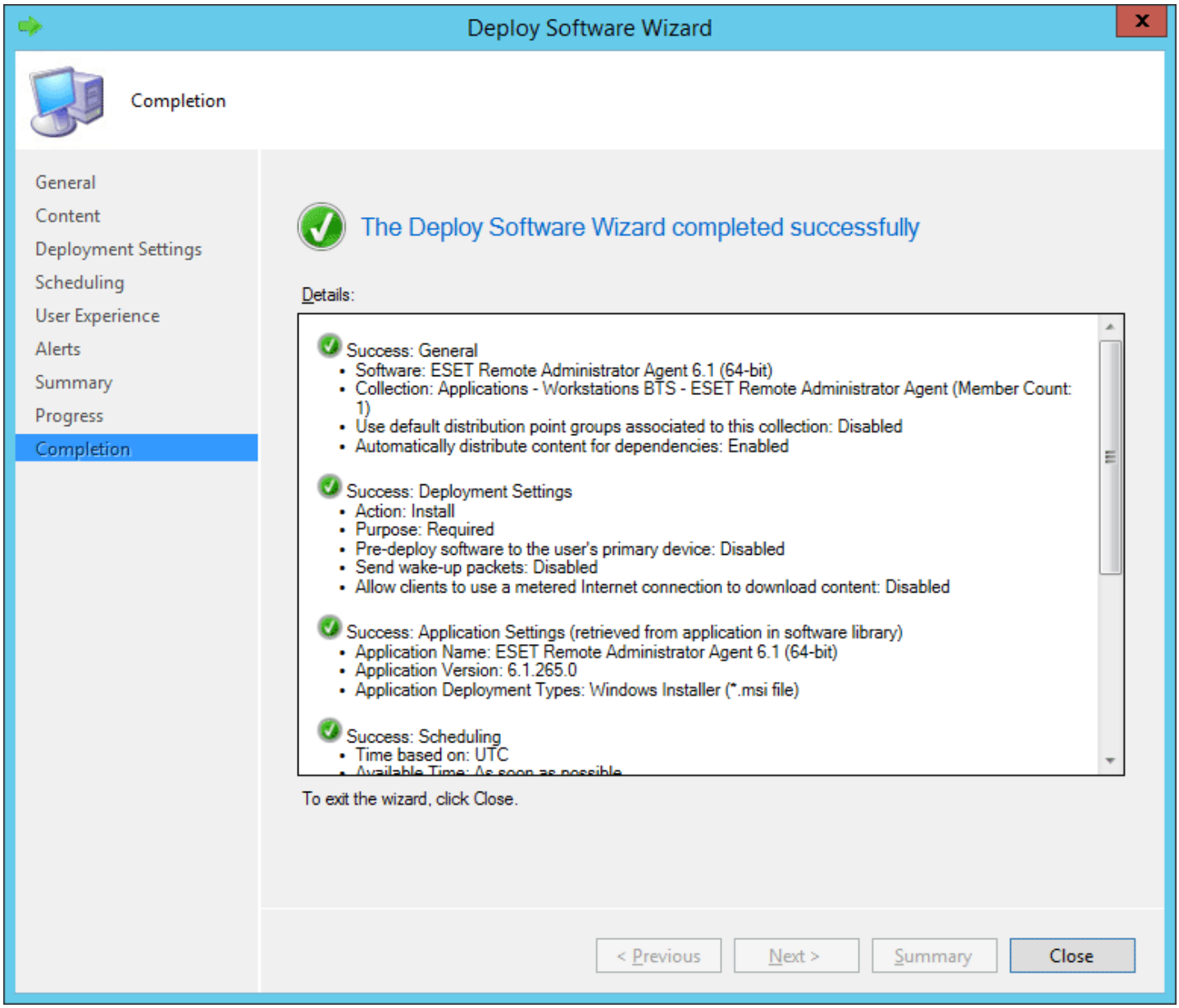

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent 6.1 (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel

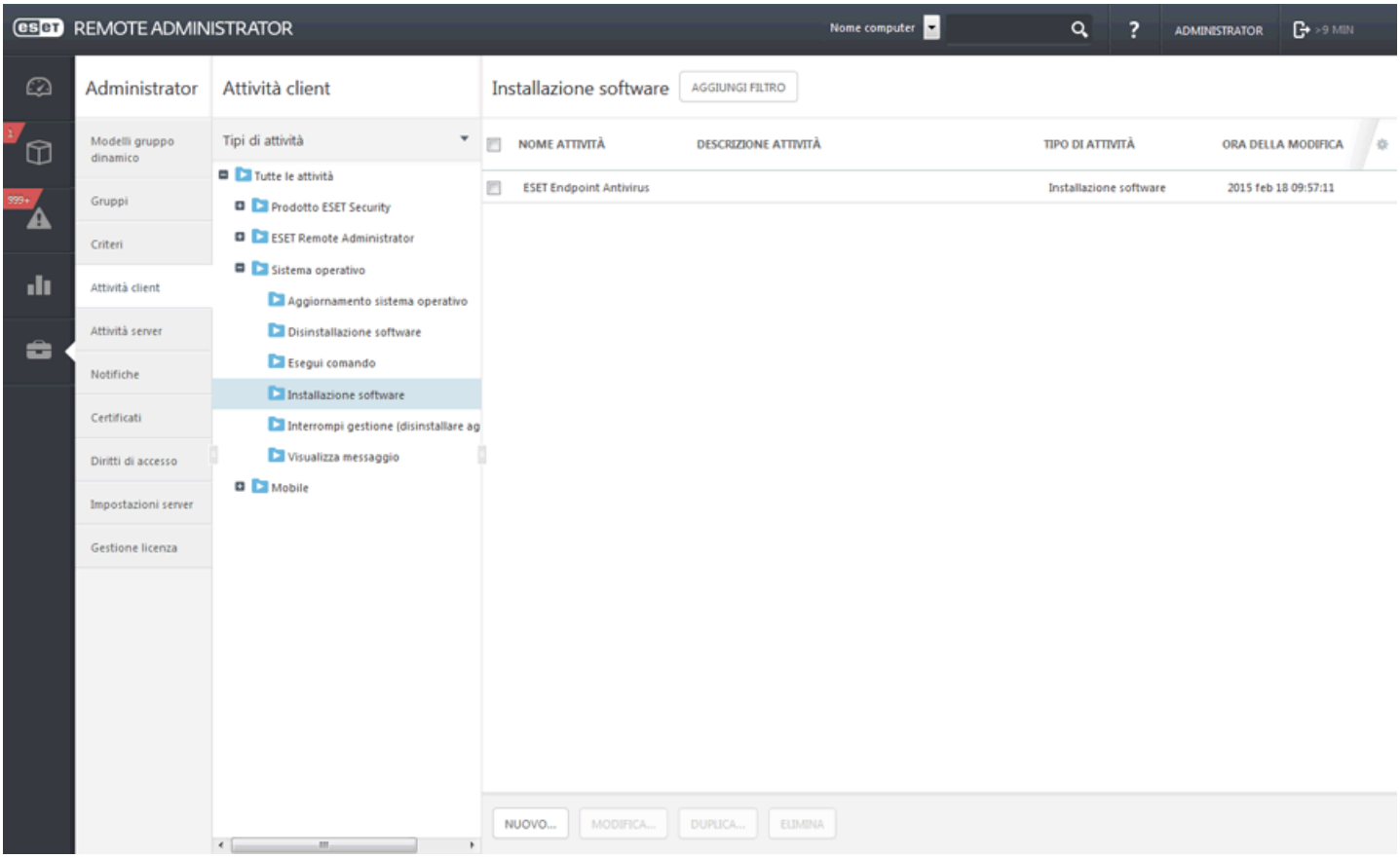

Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Completion
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
The Deploy Software Wizard completed successfully
Details:
Success: General
Software: ESET Remote Administrator Agent 6.1 (64-bit)
Collection: Applications - Workstations BTS - ESET Remote Administrator Agent (Member Count: 1)
Use default distribution point groups associated to this collection: Disabled
Automatically distribute content for dependencies: Enabled
Success: Deployment Settings
Action: Install
Purpose: Required
Pre-deploy software to the user's primary device: Disabled
Send wake-up packets: Disabled
Allow clients to use a metered Internet connection to download content: Disabled
Success: Application Settings (retrieved from application in software library)
Application Name: ESET Remote Administrator Agent 6.1 (64-bit)
Application Version: 6.1.265.0
Application Deployment Types: Windows Installer (*.msi file)
Success: Scheduling
Time based on: UTC
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

4.4.4 Installazione prodotto

I prodotti di protezione ESET possono essere installati da remoto facendo clic sulla macchina desiderata e scegliendo **Nuovo**, o creando una nuova attività di **Installazione software** nel menu **Amministrazione** > **Attività client**. Fare clic su **Nuova...** per avviare la configurazione della nuova attività.

- Utilizzare le istruzioni che seguono oppure guardare il video illustrativo della Knowledge Base.

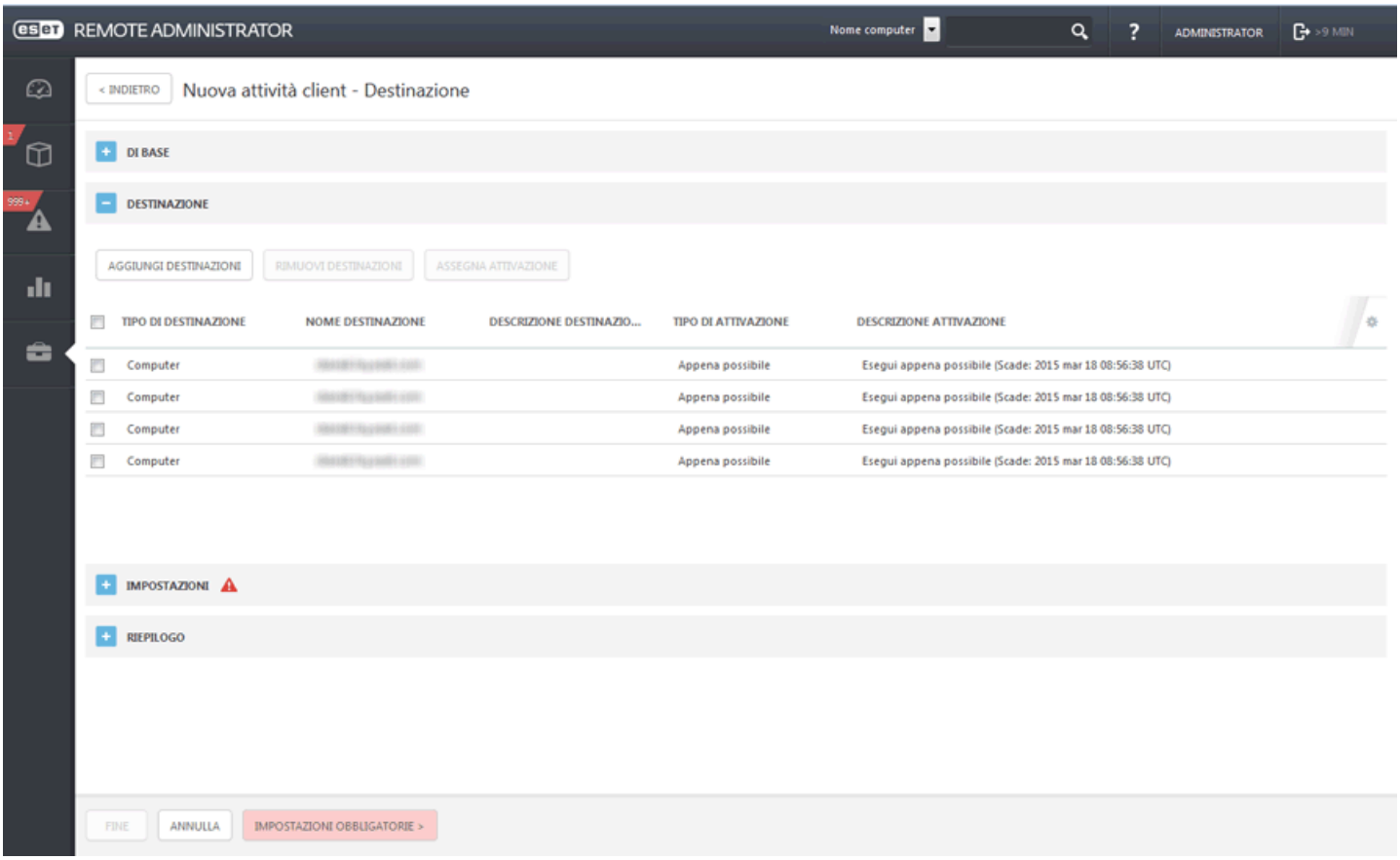


Di base

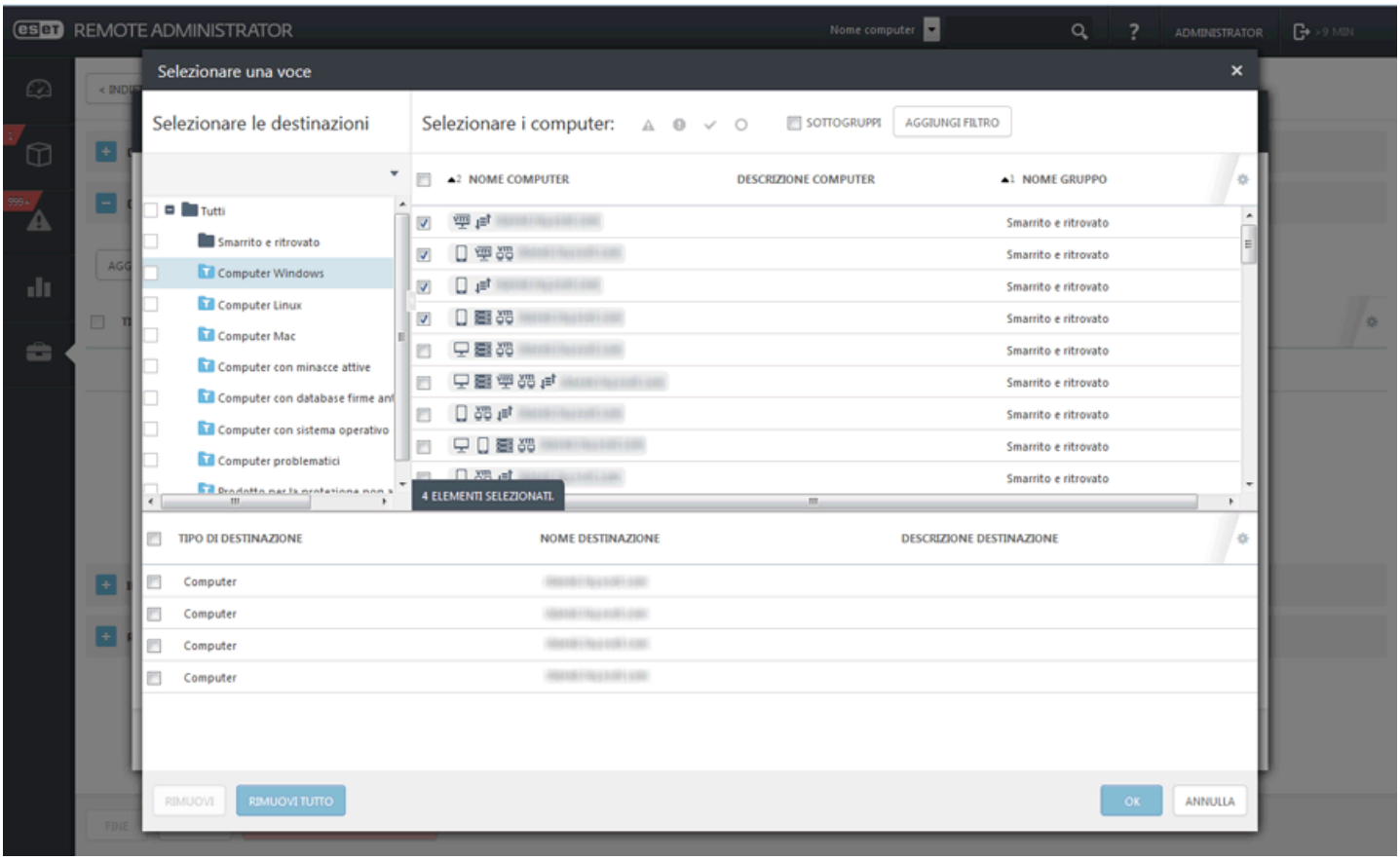
Inserire le informazioni di base sull'attività, come il **Nome**, la **Descrizione** facoltativa e il **Tipo di attività**. Il **Tipo di attività** (vedere l'elenco indicato in precedenza) definisce le impostazioni e il comportamento dell'attività. Selezionare l'attività **Installazione software**, quindi fare clic su **Destinazione**.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.

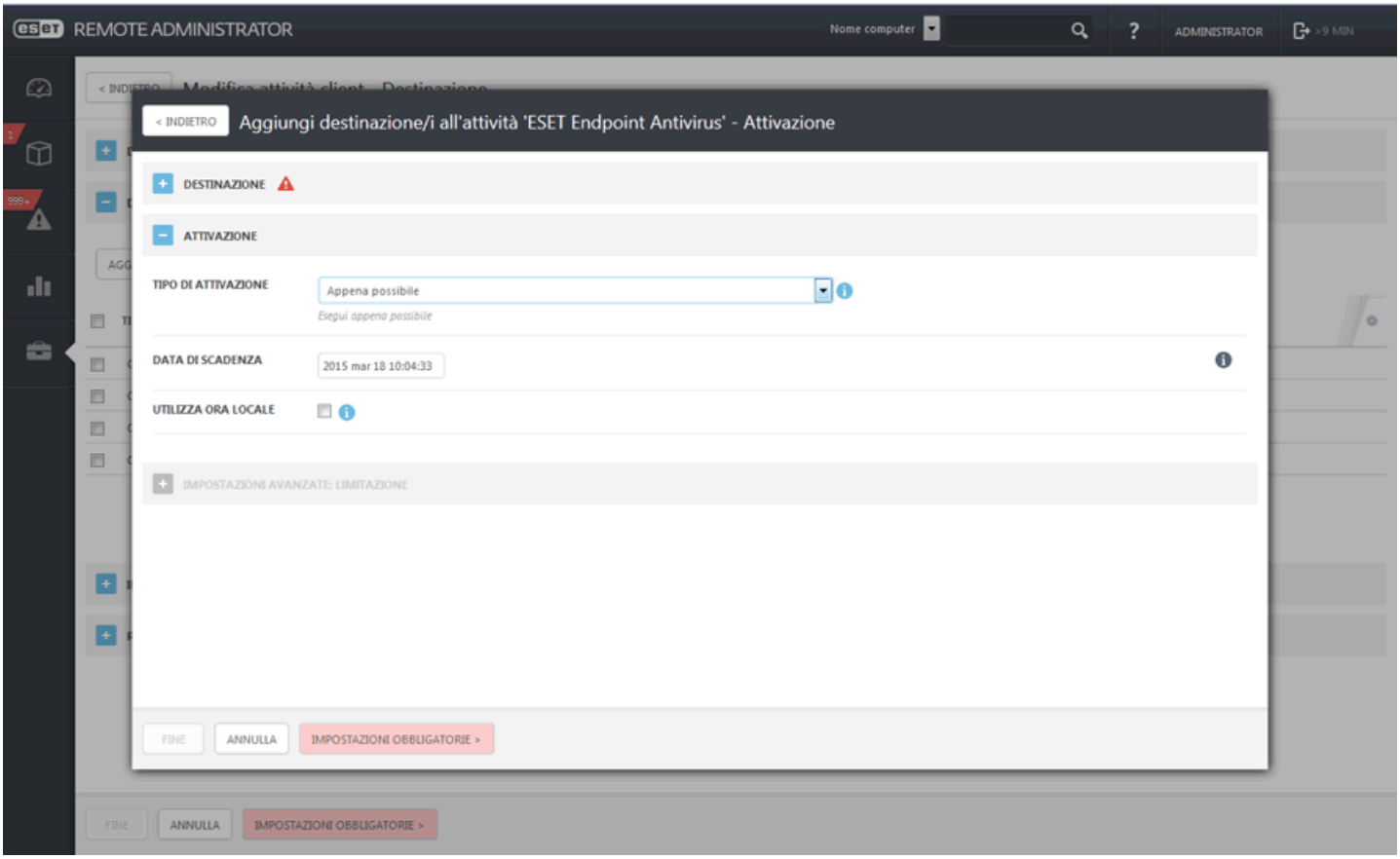


Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Attivazione

Come **Attivazione**, selezionare Esegui appena possibile. Tale operazione consentirà di inviare immediatamente l'attività ai client. L'opzione **Utilizza ora locale** fa riferimento all'ora locale del/i client e non del server.



Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per il momento, lasciare invariata l'opzione Limitazione delle richieste e fare clic su Fine per creare la nuova attività.

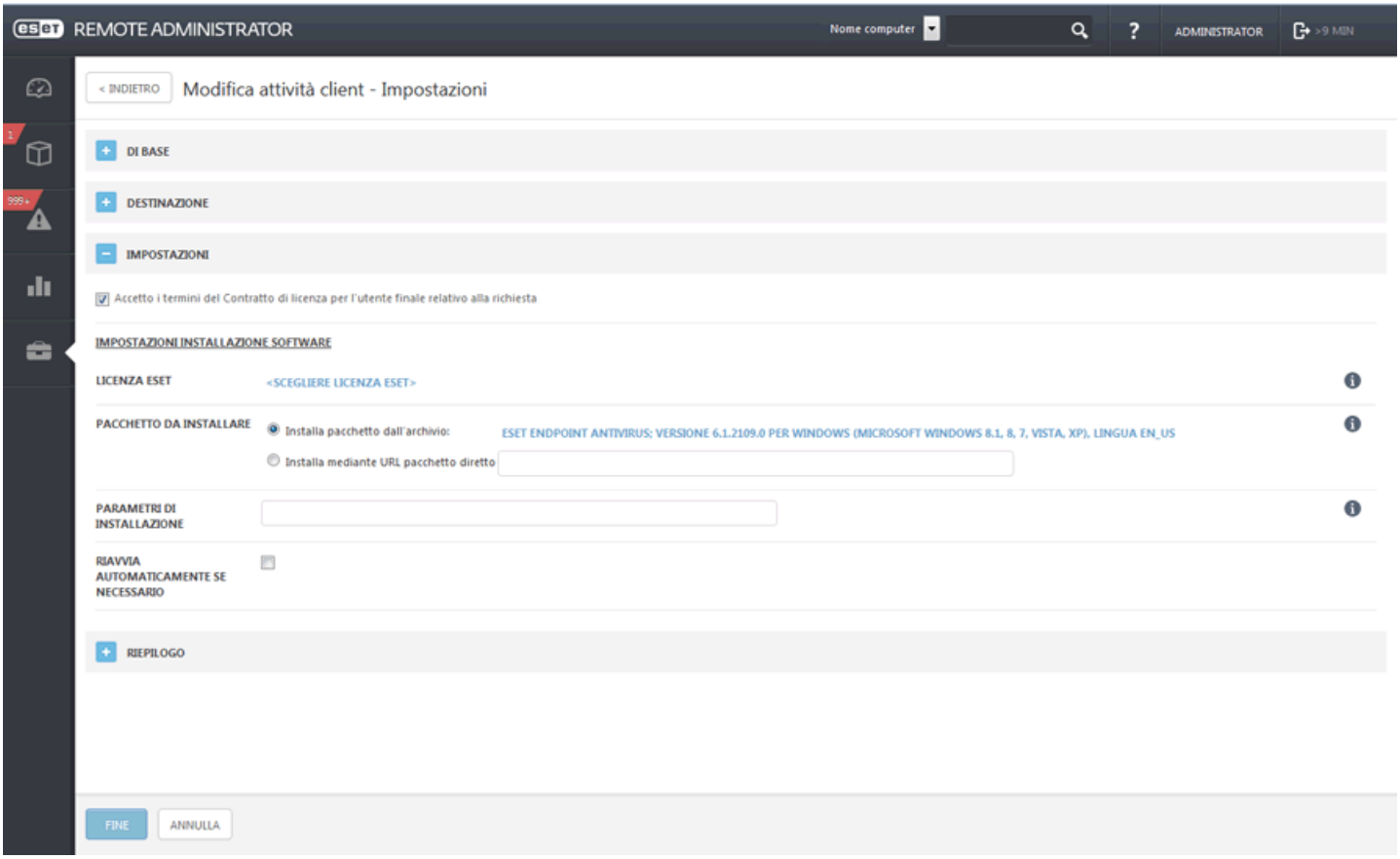
Impostazioni

Fare clic su **<Scegliere licenza ESET>** e selezionare la licenza appropriata per il prodotto installato nell'elenco di licenze disponibili. Se d'accordo, selezionare la casella di controllo accanto a **Accetto i termini del Contratto di licenza per l'utente finale relativo alla richiesta**. Per ulteriori informazioni, consultare il capitolo Gestione licenza o EULA.

Fare clic su **<Scegli pacchetto>** per selezionare un pacchetto del programma di installazione dall'archivio oppure specificare un URL del pacchetto. Verrà visualizzato un elenco di pacchetti disponibili tra cui scegliere il prodotto ESET che si desidera installare (ad esempio, ESET Endpoint Security). Selezionare il pacchetto del programma di installazione desiderato, quindi fare clic su **OK**. Se si desidera specificare l'URL del pacchetto di installazione, è necessario digitarlo o copiarlo e incollarlo nel campo di testo (non utilizzare un URL che richiede l'autenticazione).

NOTA: si tenga presente che sia il server sia l'agente necessitano dell'accesso a Internet per poter accedere all'archivio ed eseguire l'installazione. Se non si dispone di un accesso a Internet, è possibile installare il software client localmente.

Se necessario, è possibile specificare i Parametri di installazione, altrimenti lasciare questo campo vuoto. Per eseguire un riavvio automatico del computer client al termine dell'installazione, selezionare la casella di controllo accanto a **Riavvia automaticamente se necessario**. In alternativa, è possibile lasciare deselezionata questa opzione e lasciare a un altro utente la decisione di riavviare il computer client.



Riepilogo

Rivedere il riepilogo delle impostazioni configurate e fare clic su **Fine**. L'attività è stata creata e verrà inviata a/i client.

4.4.4.1 Installazione prodotto (riga di comando)

Le impostazioni che seguono sono state concepite per essere utilizzate **esclusivamente con il livello ridotto, di base e nessuno** dell'interfaccia utente. Consultare la documentazione per ulteriori informazioni sulla versione msiexec utilizzata per le opzioni corrette della riga di comando.

APPDIR="<path>"

• path: percorso della directory valido
• Directory di installazione dell'applicazione.

APPDATADIR="<path>"

• path: percorso della directory valido
• Directory di installazione dei dati dell'applicazione.

MODULEDIR="<path>"

• path: percorso della directory valido
• Directory di installazione del modulo.

ADDLOCAL="<list>"

• Installazione dei componenti: elenco di funzioni non obbligatorie da installare localmente.
• consultare http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0: disattivata, 1: attivata
• PUA

CFG_LIVEGRID_ENABLED=1/0
• 0: disattivato, 1: attivato
• LiveGrid

CFG_REPORTING_ENABLED=1/0
• 0: disattivato, 1: attivato
• Report dati di utilizzo anonimo LiveGrid

CFG_PCU_UPDATE_MODE=40/36/34
• 34: chiedi, 36: sempre, 40: mai
• Modalità dell'aggiornamento dei componenti del programma.

CFG_FIRSTSCAN_ENABLE=1/0
• 0: disattiva, 1: attiva
• Pianifica un nuovo PrimoControllo in seguito all'installazione.

CFG_EPFW_MODE=0/1/2/3
• 0: automatico, 1: interattivo, 2: criterio, 3: riconoscimento

CFG_PROXY_ENABLED=0/1
• 0: disattivato, 1: attivato

CFG_PROXY_ADDRESS=<ip>
• Indirizzo IP proxy.

CFG_PROXY_PORT=<porta>
• Numero della porta del proxy.

CFG_PROXY_USERNAME="<utente>"
• nome utente per l'autenticazione.

CFG_PROXY_PASSWORD="<pass>"
• Password per l'autenticazione.

4.4.4.2 Elenco di problemi quando l'installazione non riesce

- Pacchetto di installazione non trovato.
- Necessaria versione più recente del servizio Windows Installer.
- È già stata installata un'altra versione o un prodotto in conflitto.
- È già in corso un'altra installazione. Completare l'installazione precedente prima di procedere con l'installazione attuale.
- Installazione o disinstallazione terminata correttamente ma è necessario un riavvio del computer.
- Attività non riuscita. Si è verificato un errore. È necessario consultare il Registro di traccia dell'agente e controllare il codice restituito dal programma di installazione.

4.5 Gestione

In queste sezioni viene illustrato come Aggiungere computer o Dispositivi mobili a gruppi. Come fare per creare un nuovo criterio e assegnarlo a un gruppo..

4.5.1 Aggiungi computer ai gruppi

È possibile aggiungere computer client ai gruppi. Tale operazione consente all'utente di preservare la struttura e l'organizzazione dei computer in base alle sue preferenze. I computer possono essere aggiunti a un gruppo statico o dinamico.

I gruppi statici vengono gestiti manualmente, mentre i gruppi dinamici vengono organizzati automaticamente in base a specifici criteri contenuti in un modello. Dopo aver inserito i computer nei gruppi, è possibile assegnare criteri, attività o impostazioni. che vengono applicati a tutti i membri dei gruppi. La correlazione tra gruppi e attività/ criteri è descritta di seguito:

Gruppi statici

I gruppi statici sono gruppi di client selezionati e configurati manualmente, i cui membri sono statici, possono essere solo aggiunti/rimossi manualmente e non sono basati su criteri dinamici.

Gruppi dinamici

I Gruppi dinamici sono gruppi di client la cui appartenenza al gruppo è determinata da criteri specifici. Se un client non soddisfa i criteri, verrà rimosso dal gruppo. I computer che soddisfano i criteri verranno aggiunti automaticamente al gruppo: da qui il nome "dinamico".

4.5.1.1 Gruppi statici

- I gruppi statici vengono utilizzati per ordinare manualmente i computer client in **gruppi** e **sottogruppi**. L'utente può creare Gruppi statici personalizzati e spostarvi i computer desiderati.
- I gruppi statici possono essere creati solo manualmente. È quindi possibile spostare manualmente i computer client in tali gruppi. Ciascun computer può appartenere solo a un gruppo statico.

Sono presenti due Gruppi statici predefiniti:

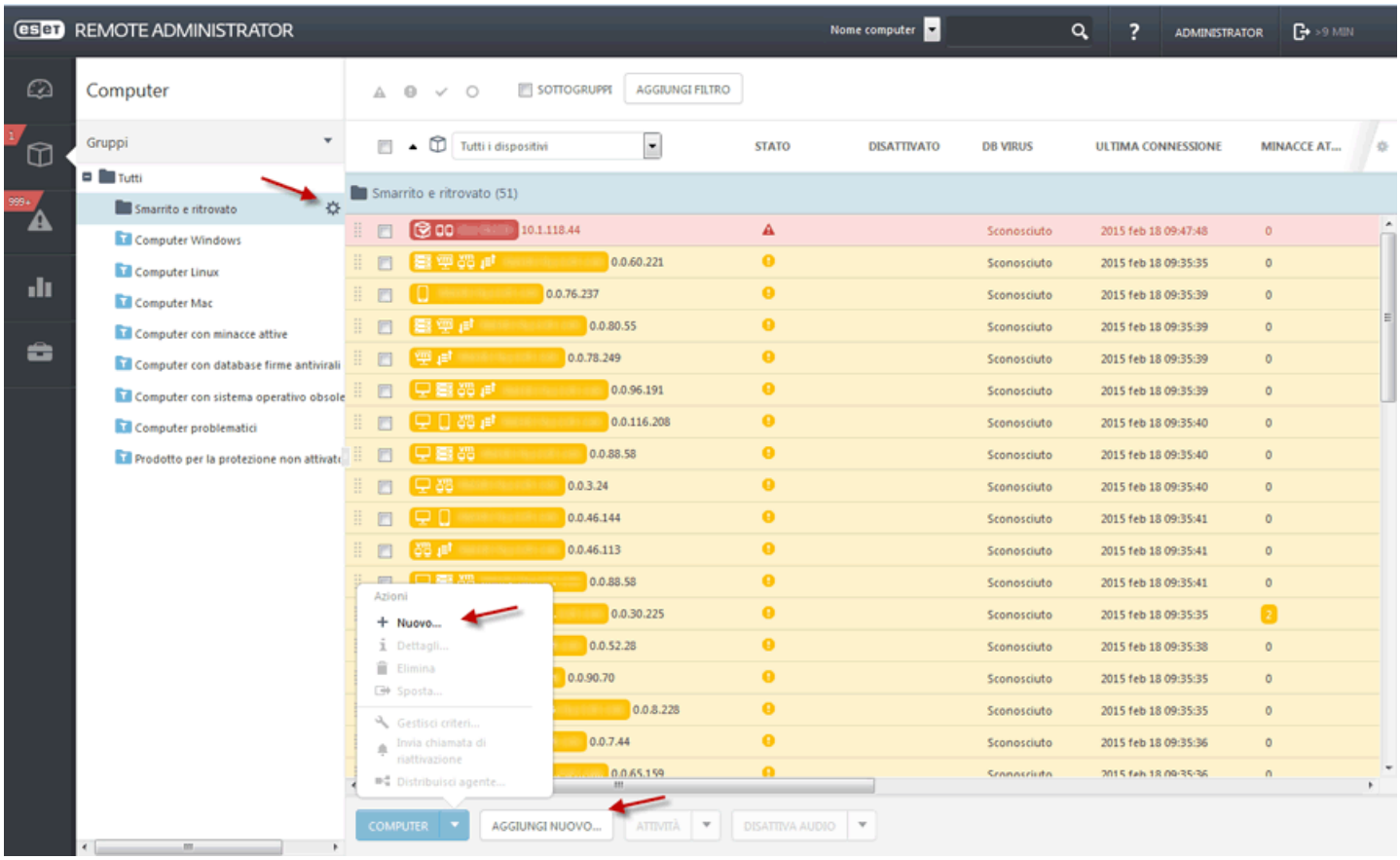
- **Tutti:** gruppo principale per tutti i computer nella rete dei server ERA. che viene utilizzato per applicare i criteri di ciascun computer come criteri predefiniti. Il gruppo viene visualizzato sempre e all'utente non è consentito modificarne il nome attraverso la modifica del gruppo stesso.
- **Smarrito e ritrovato** come gruppo figlio del gruppo **Tutti**: ciascun nuovo computer che connette per la prima volta l'agente al server viene visualizzato automaticamente in questo gruppo. Il gruppo può essere rinominato e copiato ma non eliminato o spostato.

È possibile creare gruppi statici nella sezione **Gruppo** della scheda **Amministrazione** facendo clic sul pulsante Gruppi e selezionando Nuovo gruppo statico.

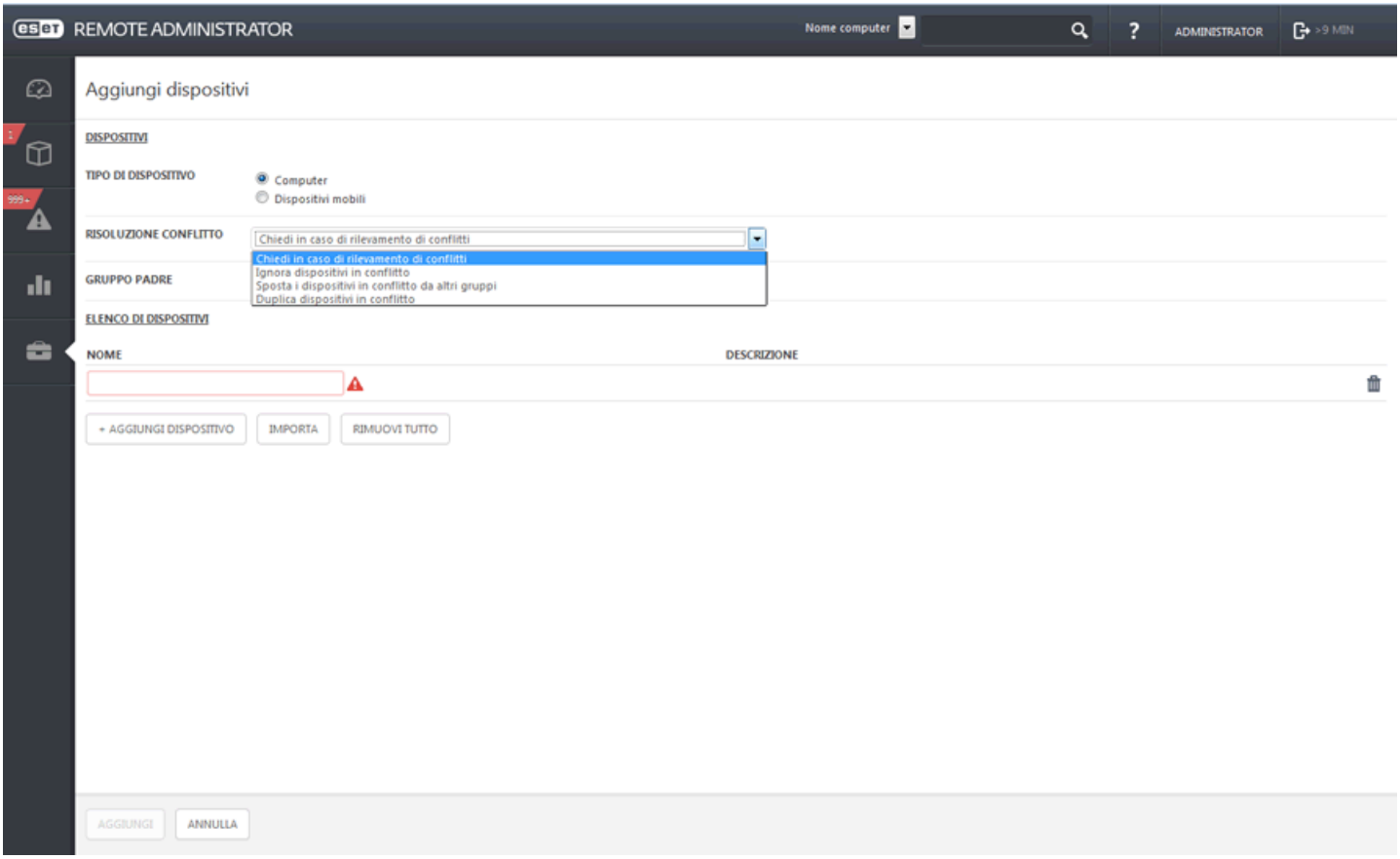
4.5.1.1.1 Aggiungi computer a un gruppo statico

Creare un nuovo gruppo statico o selezionare uno dei gruppi statici predefiniti.

Nella **scheda** Computer è possibile aggiungere nuovi computer in base a tre diverse modalità. Ad esempio, selezionare un gruppo statico: fare clic sull'icona a forma di rotella e selezionare **+ Aggiungi nuovo**.



Immettere il nome del computer che si desidera aggiungere nel campo **Nome**. Fare clic su + Aggiungi dispositivo per aggiungere altri computer oppure su Importa per importare un file contenente un elenco di computer da aggiungere. Facoltativamente, inserire una **descrizione** dei computer.



Utilizzare il menu a discesa Risoluzione conflitto per selezionare l'azione da eseguire se un computer che si sta aggiungendo esiste già in ERA:

Chiedi in caso di rilevamento di conflitti: in caso di rilevamento di un conflitto, il programma chiederà all'utente di selezionare un'azione (vedere le opzioni sottostanti).
Ignora computer in conflitto: I computer duplicati non verranno aggiunti.
Sposta i computer in conflitto da altri gruppi: i computer in conflitto verranno spostati dai gruppi originali al gruppo **Tutti**.
Duplica computer in conflitto: verranno aggiunti nuovi computer, ma con nomi diversi.

Fare clic su **Aggiungi**. È possibile visualizzare i computer nell'elenco sulla destra dopo aver selezionato il relativo gruppo di appartenenza.

NOTA: l'aggiunta di computer multipli potrebbe richiedere più tempo. Potrebbe essere eseguita una ricerca DNS inversa.

Per ulteriori informazioni sulle modalità di aggiunta dei dispositivi mobili, consultare il capitolo Registrazione dispositivi mobili.

4.5.1.2 Gruppi dinamici

Ogni gruppo dinamico utilizza un modello per filtrare i computer client. Una volta definito, un modello può essere utilizzato in altri Gruppi dinamici per filtrare i client. ERA prevede vari modelli di Gruppi dinamici predefiniti e pronti all'uso per semplificare la categorizzazione dei computer client.

I Gruppi dinamici sono gruppi di client selezionati in base a criteri specifici. Se un computer client non soddisfa i criteri, verrà rimosso dal gruppo. In caso di soddisfacimento delle condizioni definite, verrà aggiunto al gruppo. La selezione dei gruppi viene eseguita automaticamente in base alle impostazioni configurate, fatta eccezione per il caso dei Gruppi statici.

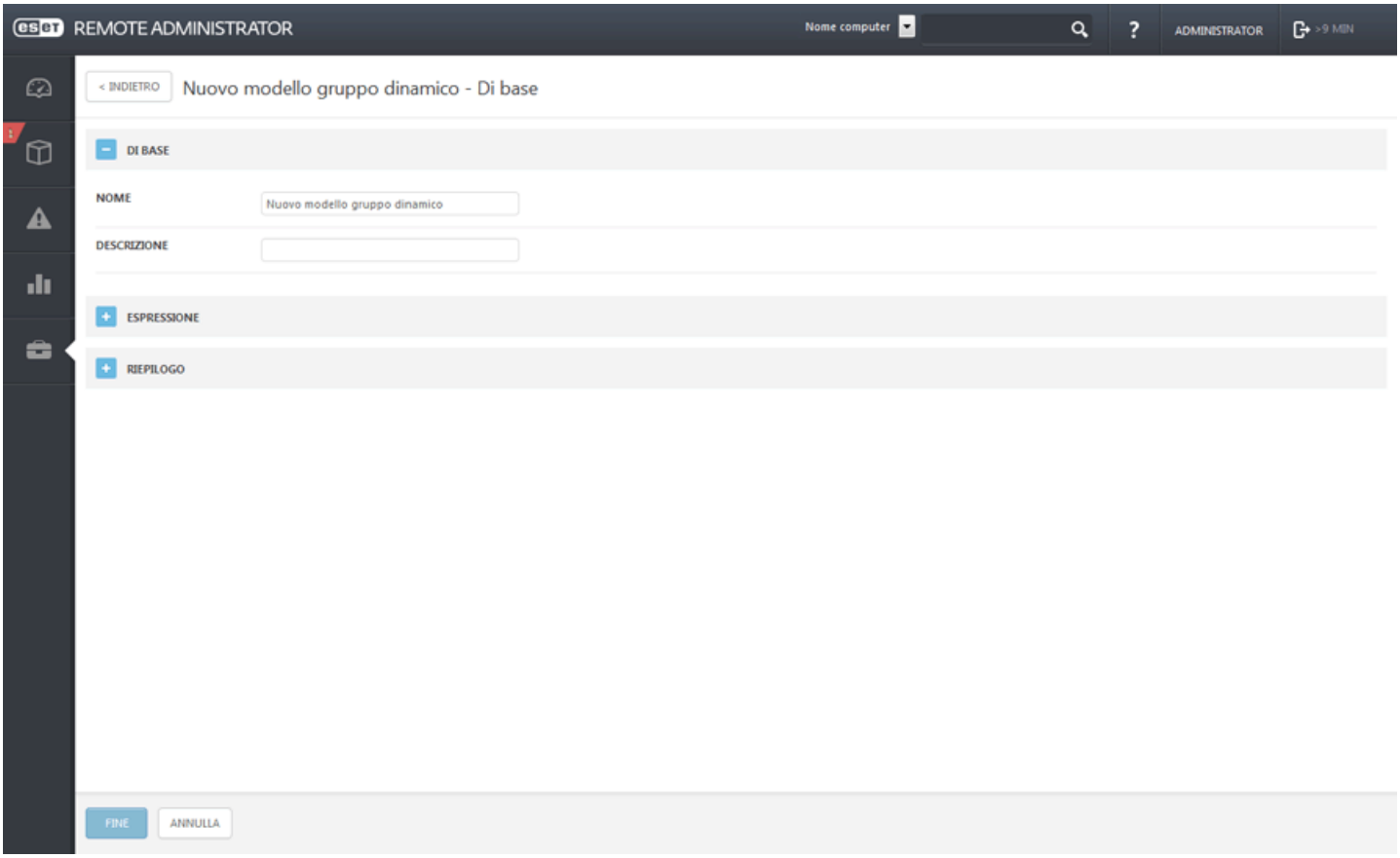
La sezione Modelli gruppi dinamici contiene modelli sia predefiniti sia personalizzati in base a criteri diversi. Tutti i modelli vengono visualizzati in un elenco. Fare clic su un modello esistente per modificarlo. Per creare un nuovo modello di gruppo dinamico, fare clic su **Nuovo modello**.

4.5.1.2.1 Nuovo modello gruppo dinamico

Fare clic su **Nuovo modello** in **Amministrazione** > **Modelli gruppi dinamici.**

Di base

1. Immettere un **Nome** e una **Descrizione** per il nuovo modello gruppo dinamico.



Espressione

Selezionare un operatore logico nel menu **Operazione**.

- **E**: tutte le condizioni definite devono essere vere.
- **O**: almeno una condizione deve essere vera.
- **NON E**: almeno una condizione deve essere falsa.
- **NON O**: tutte le condizioni devono essere false.

Ad esempio, selezionare **E**. Ciò significa che un computer deve soddisfare tutte le condizioni per poter apparire in un Gruppo dinamico che utilizza questo modello.

- Fare clic su **+ Aggiungi regola** e selezionare una condizione. ad esempio per i client che utilizzano i computer portatili collegati alla rete elettrica. Selezionare **Hardware** > **Alimentazione a batteria** > **=(uguale)** > **Non in esaurimento**.
- Fare clic su **+ Aggiungi regola** per immettere una seconda condizione (il numero di regole non è limitato). Selezionare **Edizione sistema operativo** > **Tipo di sistema operativo** > **=(uguale)** > **Windows 8.1** (immettere questo valore nel campo vuoto).

Se entrambe le suddette condizioni sono soddisfatte, il client apparirà nel Gruppo dinamico.

Riepilogo

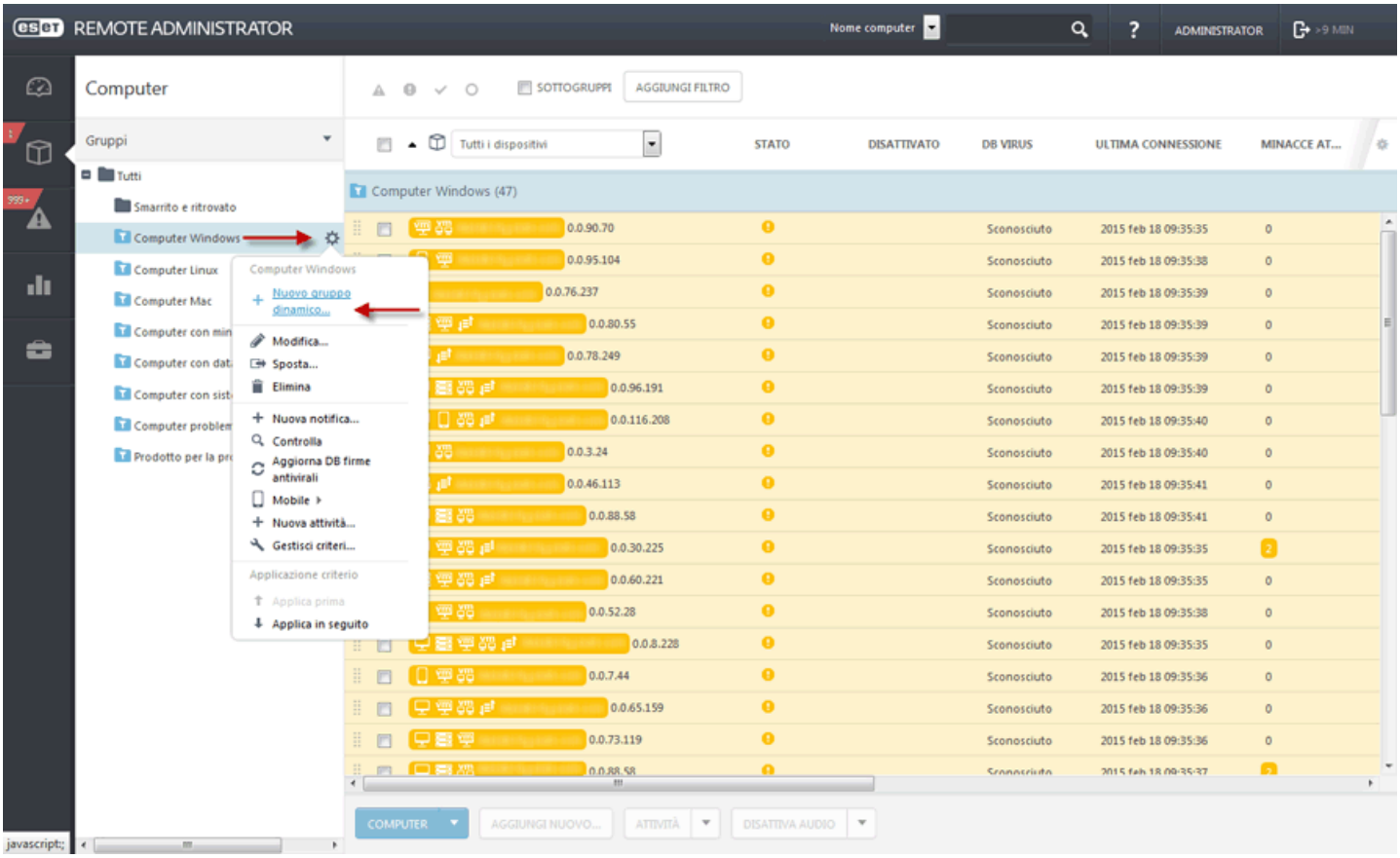
Rivedere le impostazioni configurate e fare clic su **Fine** per creare il modello. Il nuovo modello verrà aggiunto all'elenco di tutti i modelli e può essere utilizzato più avanti per creare un nuovo gruppo dinamico. Nelle opzioni **Espressione** è possibile configurare le regole/condizioni per il gruppo (l'editor regole è descritto qui). Ora ogni gruppo dinamico basato su questo modello valuterà tali regole.

Per salvare le modifiche, fare clic su **Fine**.

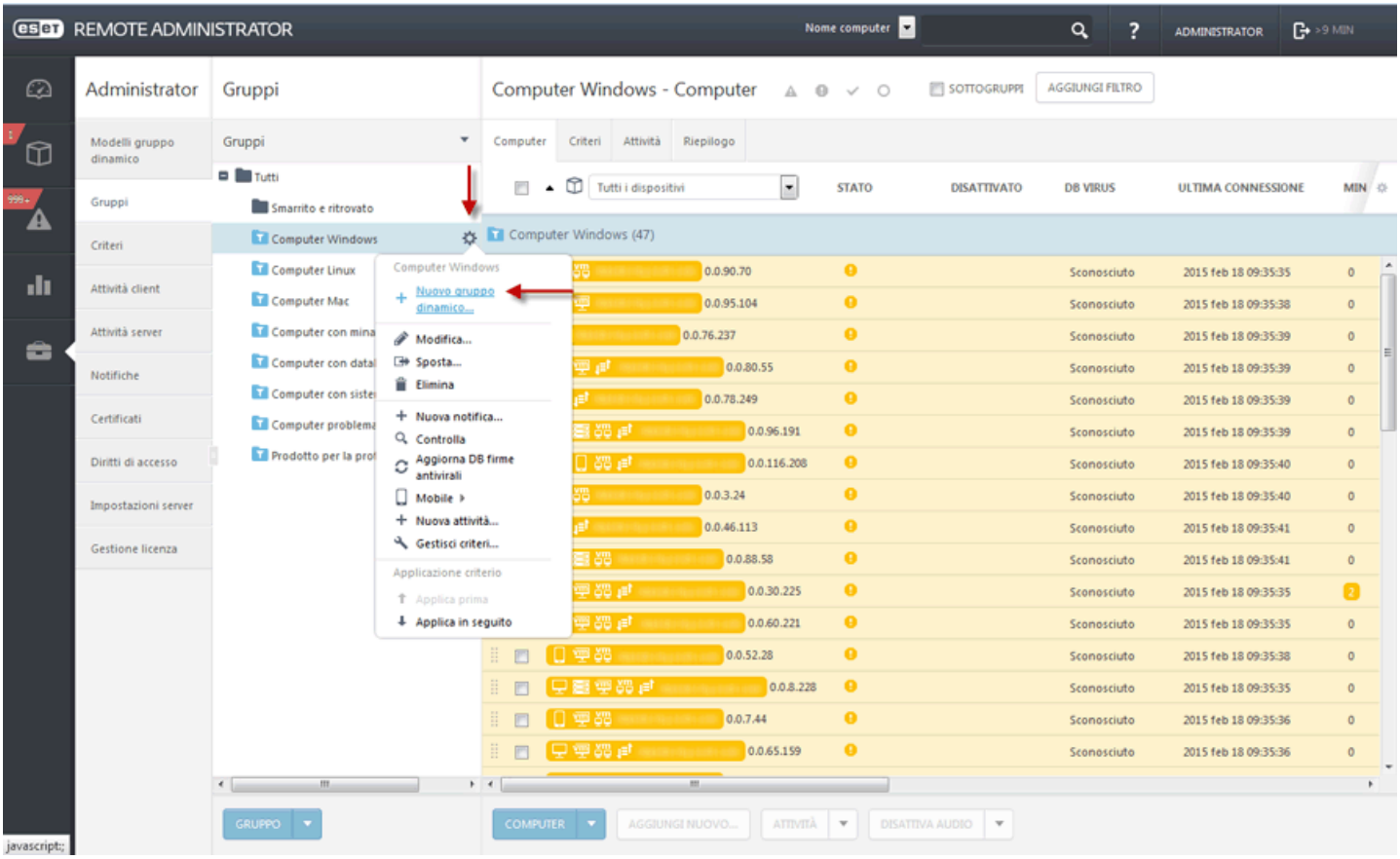
4.5.1.2.2 Crea nuovo gruppo dinamico

Per creare un nuovo gruppo dinamico, è possibile utilizzare una delle tre seguenti modalità:

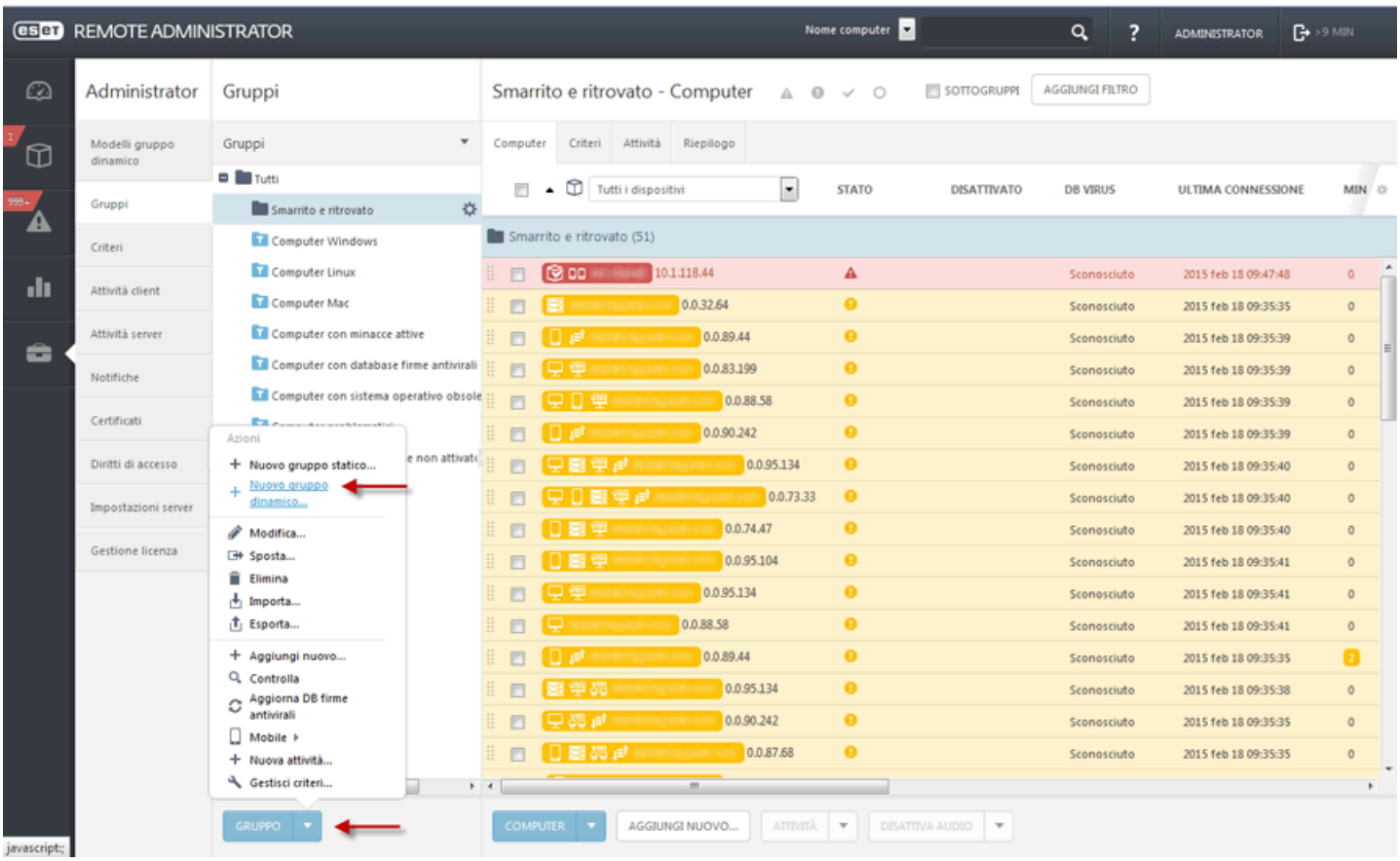
1. Fare clic su **Computer** > **Gruppi** > ⚙ e selezionare **Nuovo gruppo dinamico...**



2. Fare clic su **Amministrazione** > **Gruppi** > ⚙ > **Nuovo sottogruppo dinamico...**



3. Fare clic su **Amministrazione** > **Gruppi** > Fare clic sul pulsante **Gruppo**, quindi su **Nuovo gruppo dinamico...**

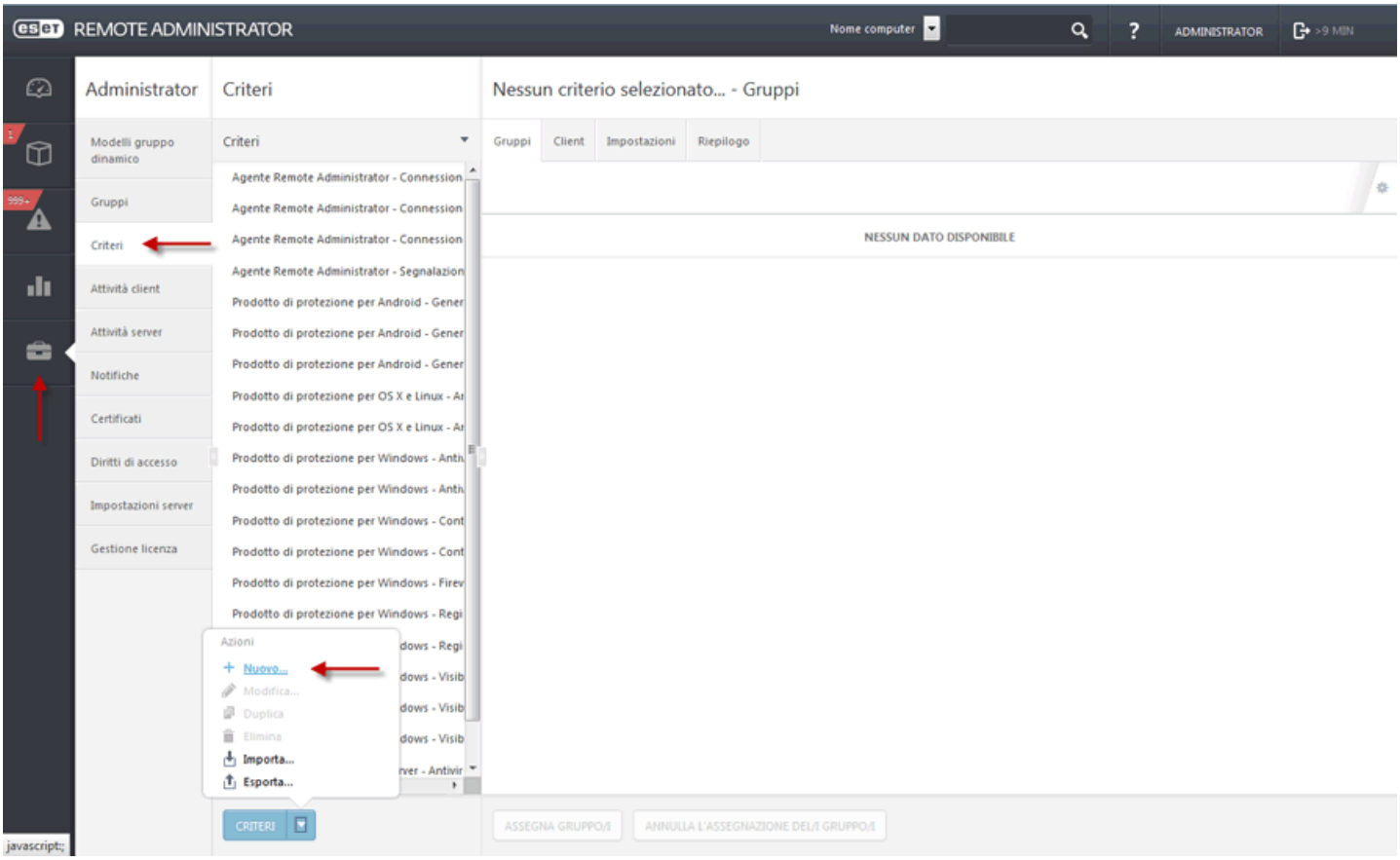


Verrà visualizzata una Procedura guidata nuovo gruppo dinamico.

4.5.2 Crea un nuovo criterio

Nell'esempio verrà creato un nuovo criterio per l'intervallo di connessione dell'agente ERA. Si consiglia vivamente di eseguire questa operazione prima di effettuare i test sulla distribuzione di massa nell'ambiente d'uso.

1. Creare un nuovo gruppo statico.
2. Aggiungere un nuovo criterio facendo clic su **Amministrazione** > **Criteri**. Fare clic su **Criteri** nella parte inferiore e selezionare **Nuovo**.

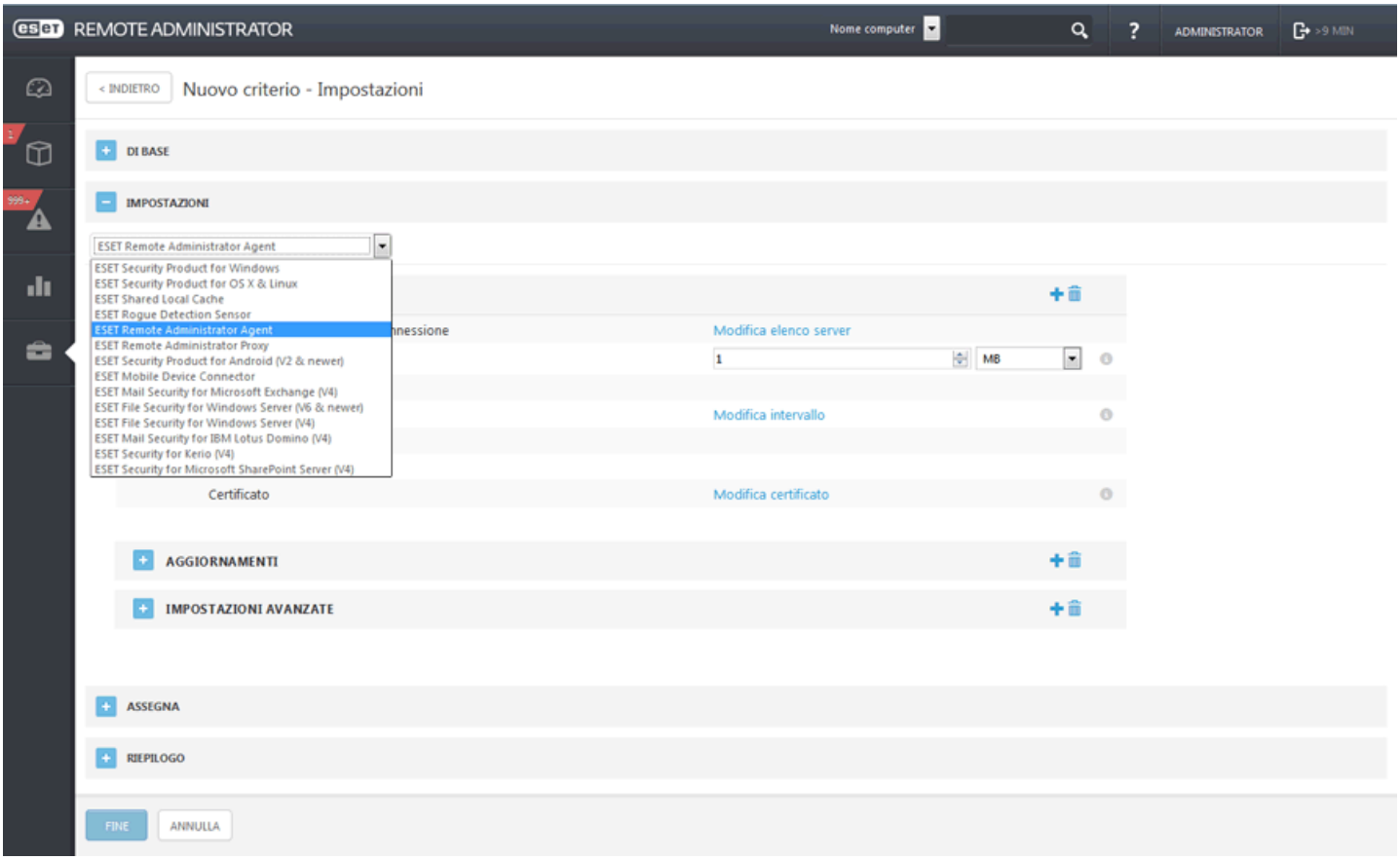


Di base

Immettere un **Nome** per il nuovo criterio (ad esempio, "Intervallo di connessione agente"). Il campo **Descrizione** è facoltativo.

Impostazioni

Selezionare **Agente ESET Remote Administrator** dal menu a discesa **Prodotto**.



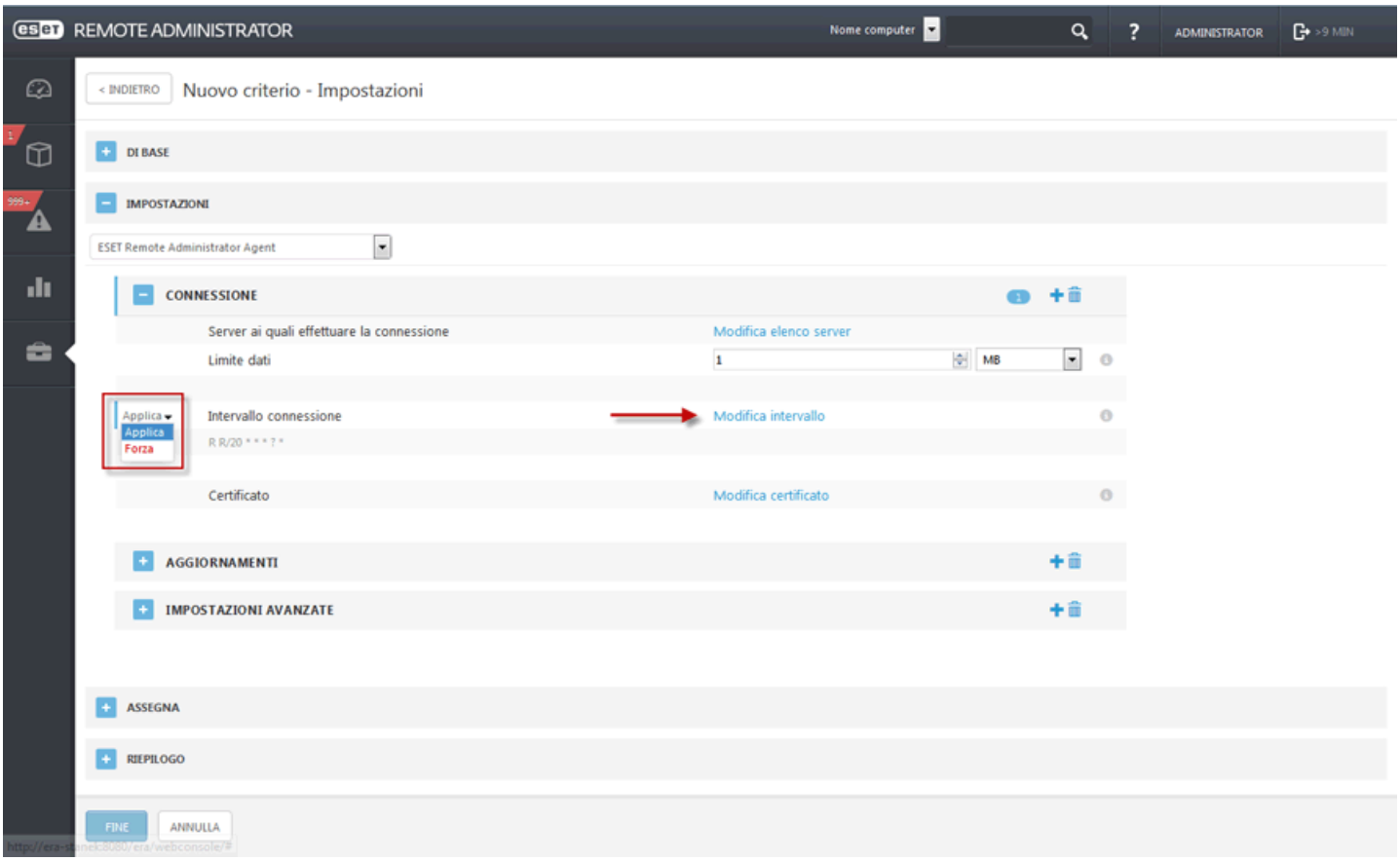
Connessione

Selezionare una categoria nella struttura ad albero sulla sinistra. Nel riquadro sulla destra, modificare le impostazioni, se necessario. Ciascuna impostazione rappresenta una regola per la quale è possibile definire un contrassegno. Per facilitare la navigazione, vengono contate tutte le regole. Il numero di regole definite dall'utente in una particolare sezione verrà visualizzato automaticamente. Sarà inoltre possibile visualizzare un numero accanto al nome di una categoria nella struttura ad albero sulla sinistra. Questa sezione consente di visualizzare una panoramica delle regole in tutte le relative sezioni. In tal modo, sarà possibile offrire all'utente una rapida panoramica del numero di impostazioni o regole definite e del punto in cui viene eseguita tale operazione.

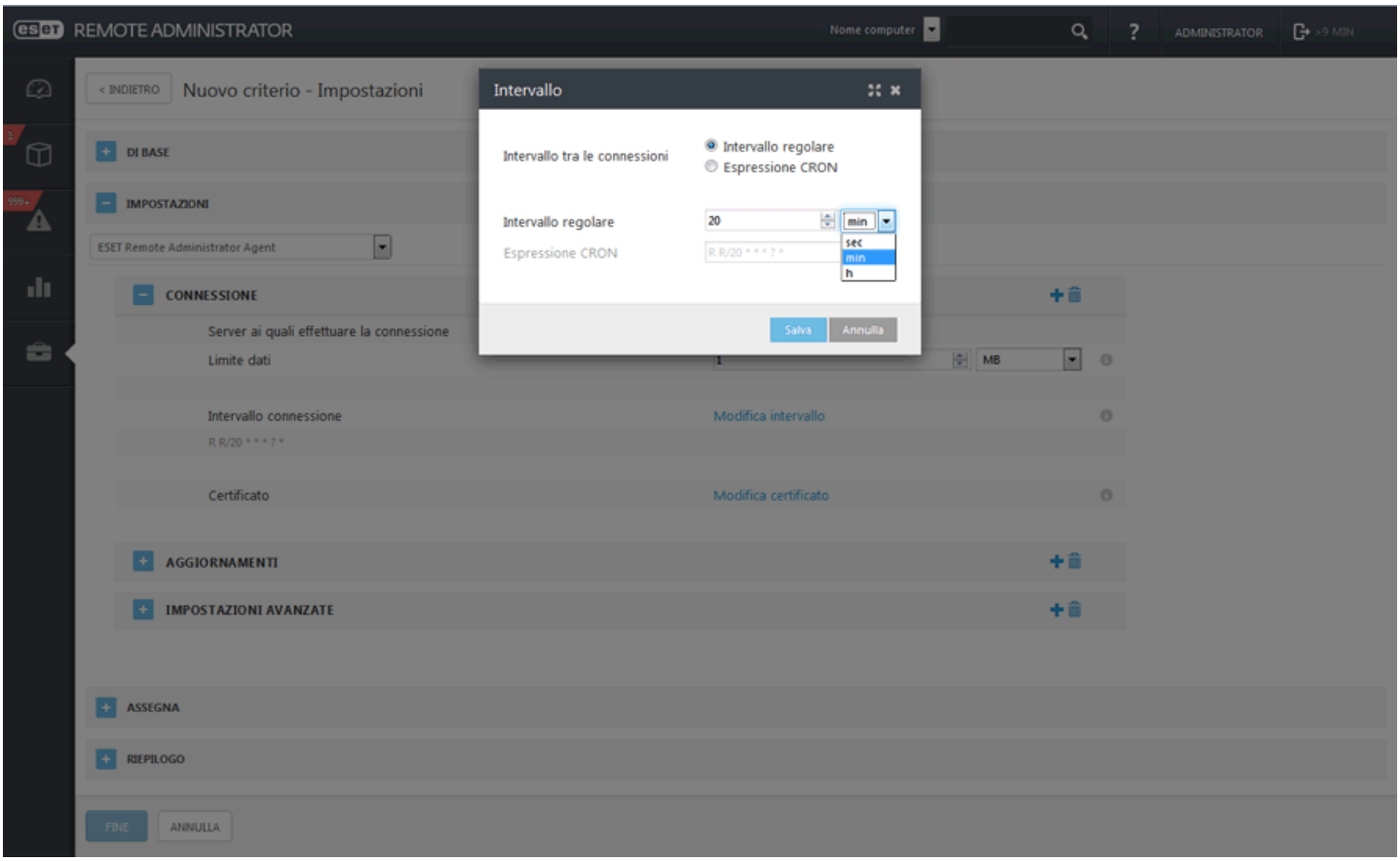
Per facilitare la modifica dei criteri, è anche possibile utilizzare i seguenti suggerimenti:

- utilizzare + per impostare il contrassegno **Applica** a tutte le voci in una sezione corrente
- eliminare le regole utilizzando l'icona del **Cestino**

Fare clic su **Modifica intervallo**.



Nel campo **Intervallo regolare**, impostare il valore dell'intervallo desiderato (si consiglia 60 secondi) e fare clic su Salva.



Dopo aver creato un nuovo criterio per l'intervallo di connessione dell'agente, assegnarlo al gruppo statico creato nel passaggio 1.

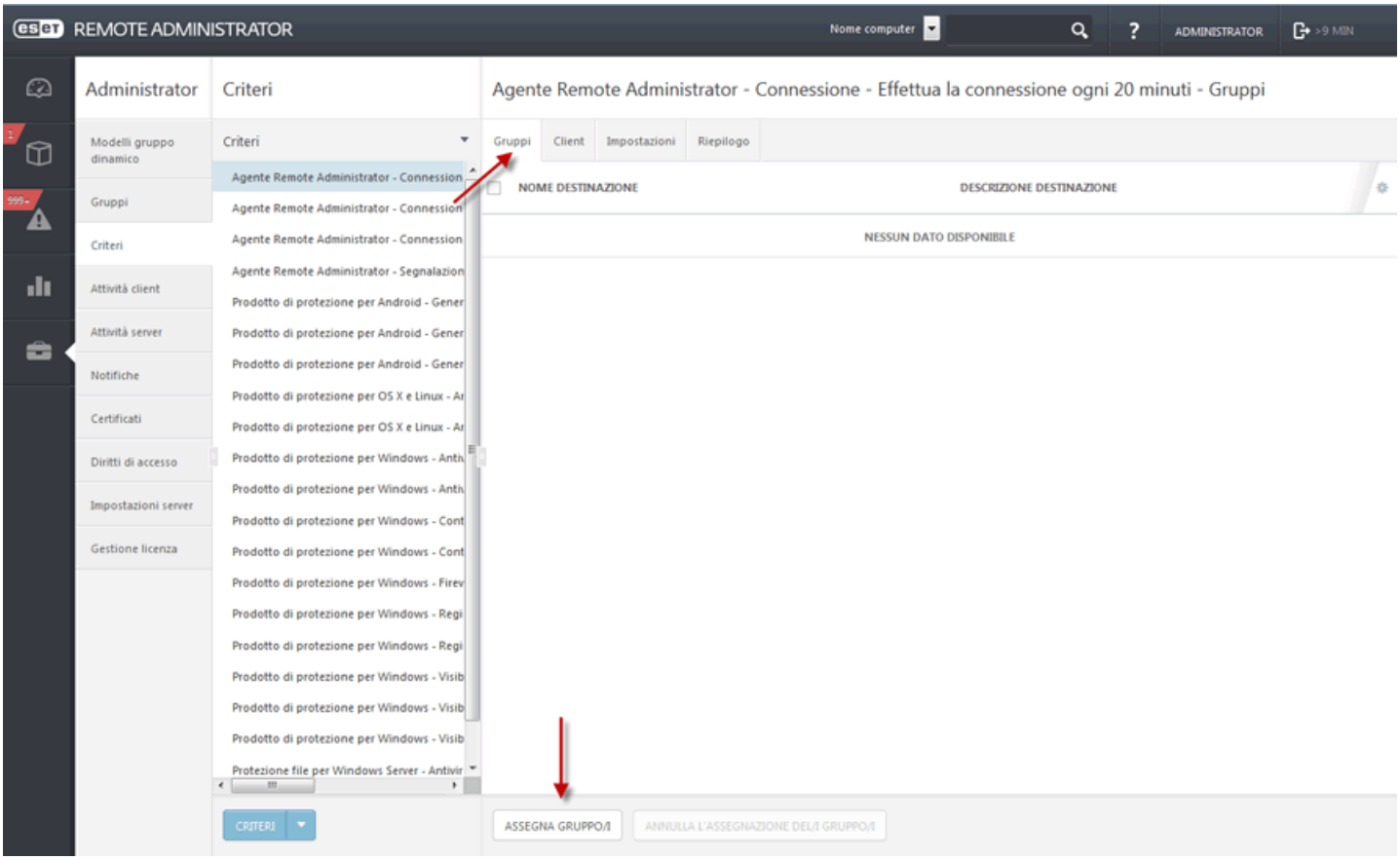
Dopo aver terminato i test sulla distribuzione di massa, modificare le impostazioni del criterio per l'intervallo di connessione dell'agente ERA create al passaggio 2.

Fare clic su **Amministrazione** > **Gruppi** e selezionare la scheda **Criteri**. Fare clic sul criterio per l'intervallo di connessione dell'agente, scegliere **Modifica**, quindi fare clic su **Impostazioni** > **Connessione**. Fare clic su **Modifica intervallo** e impostare l'intervallo di connessione su 20 minuti.

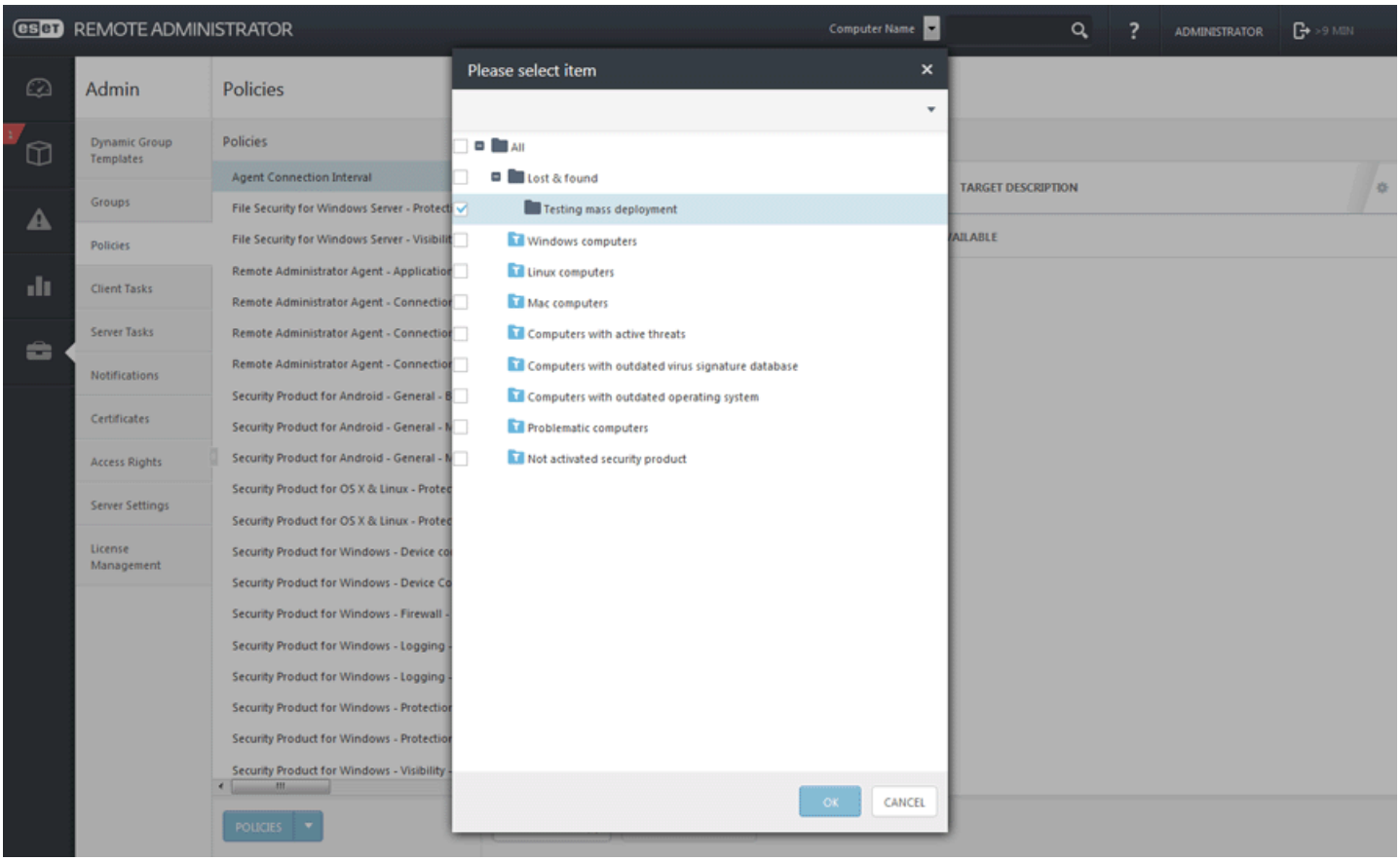
4.5.3 Assegna un criterio a un gruppo

Dopo aver creato un criterio, l'utente può assegnarlo a un **Gruppo statico** o **dinamico**. Un criterio può essere assegnato in due modi:

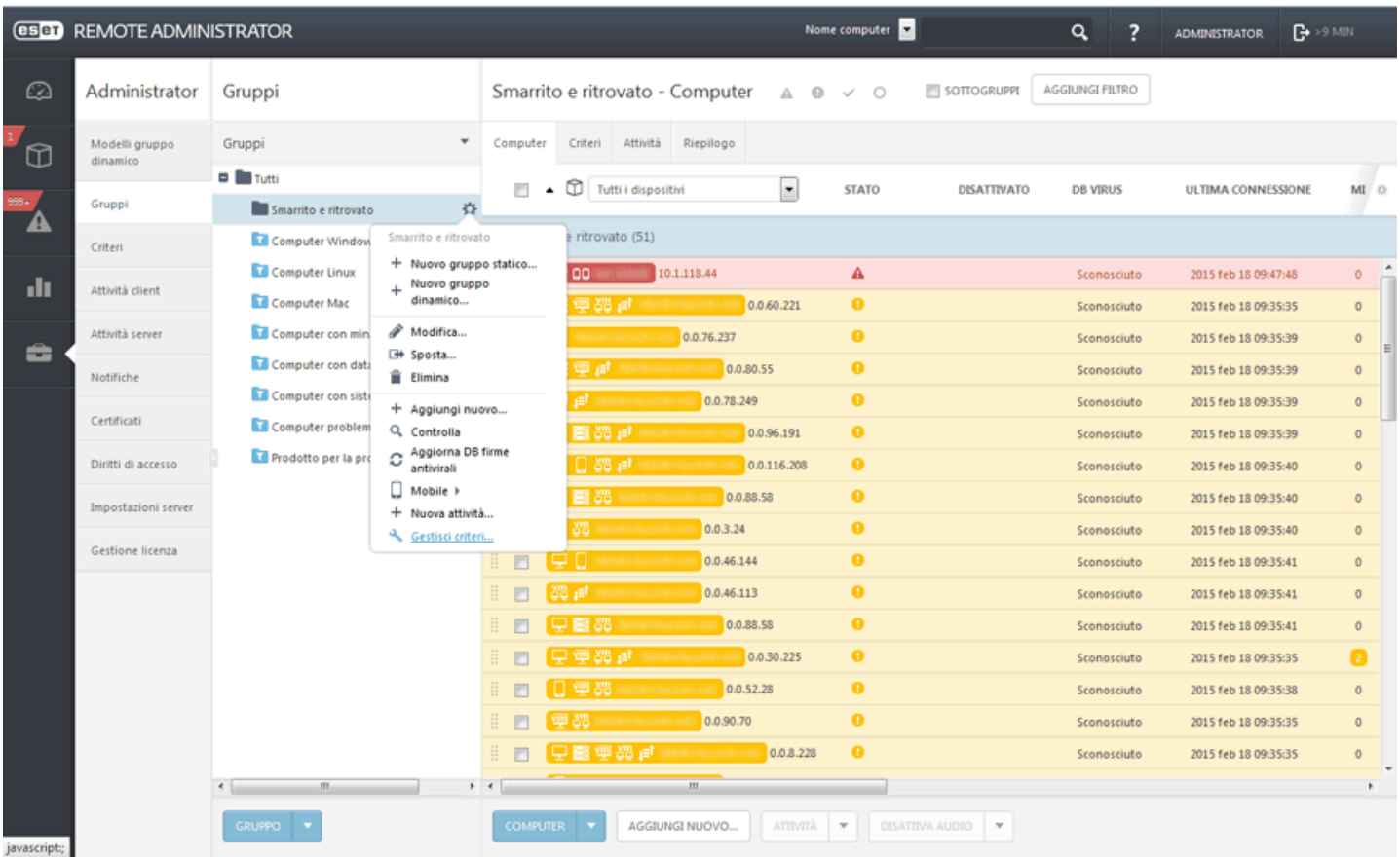
1. In **Amministrazione** > **Criteri** > selezionare un criterio e fare clic su **Assegna gruppo/i**. Selezionare un gruppo statico o dinamico e fare clic su **OK**.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Criteri
Agente Remote Administrator - Connessione - Effettua la connessione ogni 20 minuti - Gruppi
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
Criteri
Agente Remote Administrator - Connessione
Agente Remote Administrator - Connessione
Agente Remote Administrator - Connessione
Agente Remote Administrator - Segnalazione
Prodotto di protezione per Android - Gener
Prodotto di protezione per Android - Gener
Prodotto di protezione per Android - Gener
Prodotto di protezione per OS X e Linux - Ar
Prodotto di protezione per OS X e Linux - Ar
Prodotto di protezione per Windows - Anti
Prodotto di protezione per Windows - Anti
Prodotto di protezione per Windows - Cont
Prodotto di protezione per Windows - Cont
Prodotto di protezione per Windows - Firev
Prodotto di protezione per Windows - Regi
Prodotto di protezione per Windows - Regi
Prodotto di protezione per Windows - Visib
Prodotto di protezione per Windows - Visib
Prodotto di protezione per Windows - Visib
Protezione file per Windows Server - Antivir
Gruppi
Client
Impostazioni
Riepilogo
NOME DESTINAZIONE
DESCRIZIONE DESTINAZIONE
NESSUN DATO DISPONIBILE
CRITERI
ASSEGNA GRUPPO/I
ANNULLA L'ASSEGNAZIONE DEL/I GRUPPO/I

Selezionare un **Gruppo** dall'elenco.



2. Fare clic su **Amministrazione** > **Gruppi** > **Gruppo** oppure sull'icona a forma di rotella accanto al nome del gruppo e selezionare **Gestisci criteri**.



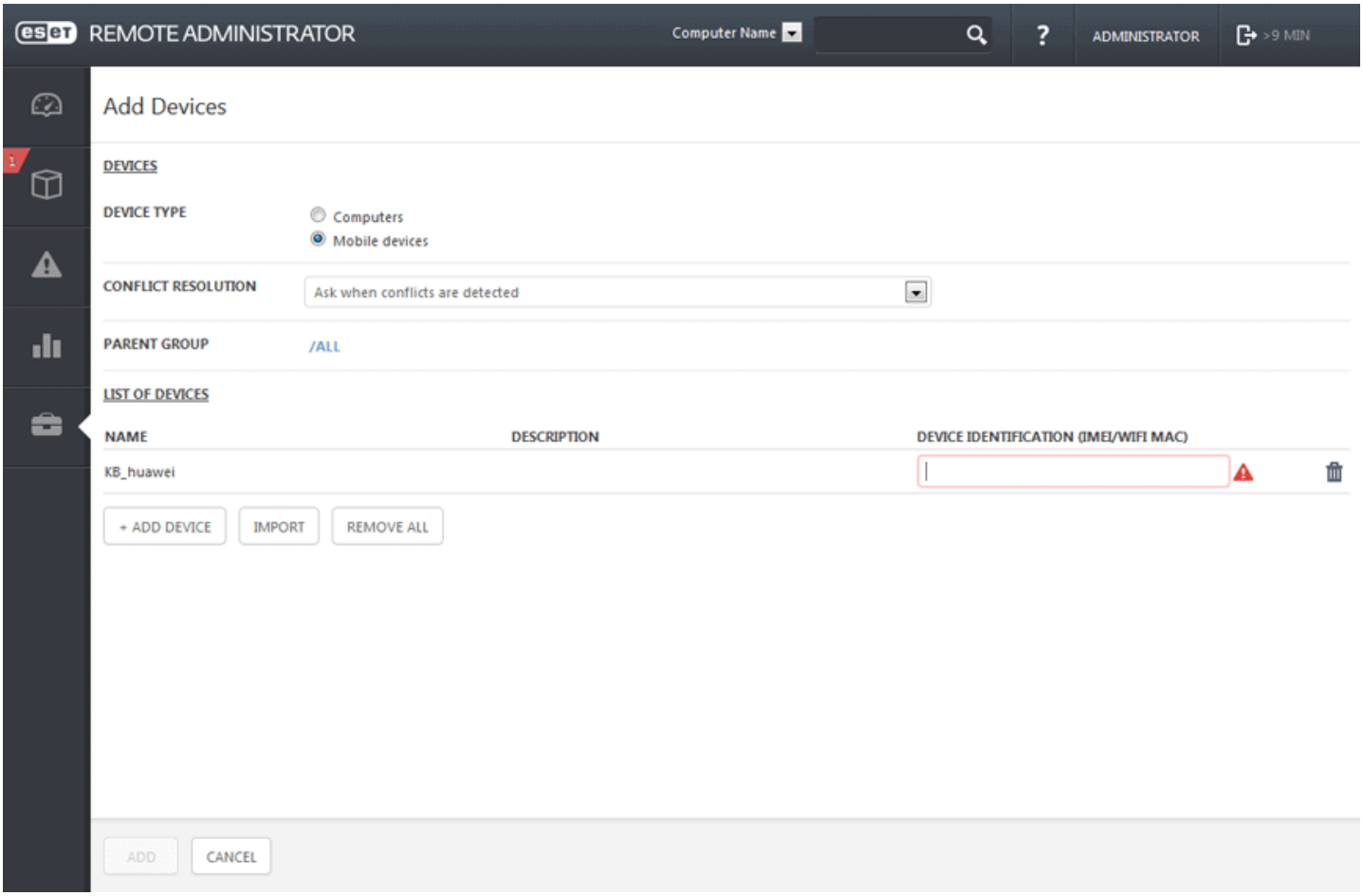
Nella finestra **Ordine applicazione criterio** fare clic su **Aggiungi criterio**. Selezionare la casella di controllo accanto al criterio che si desidera assegnare al gruppo e fare clic su **OK**.
Fare clic su **Salva**. Per visualizzare i criteri assegnati a un gruppo specifico, selezionarlo e fare clic sulla scheda **Criteri** per aprire un elenco di criteri assegnati al gruppo.

NOTA: per ulteriori informazioni sui criteri, consultare il capitolo Criteri.

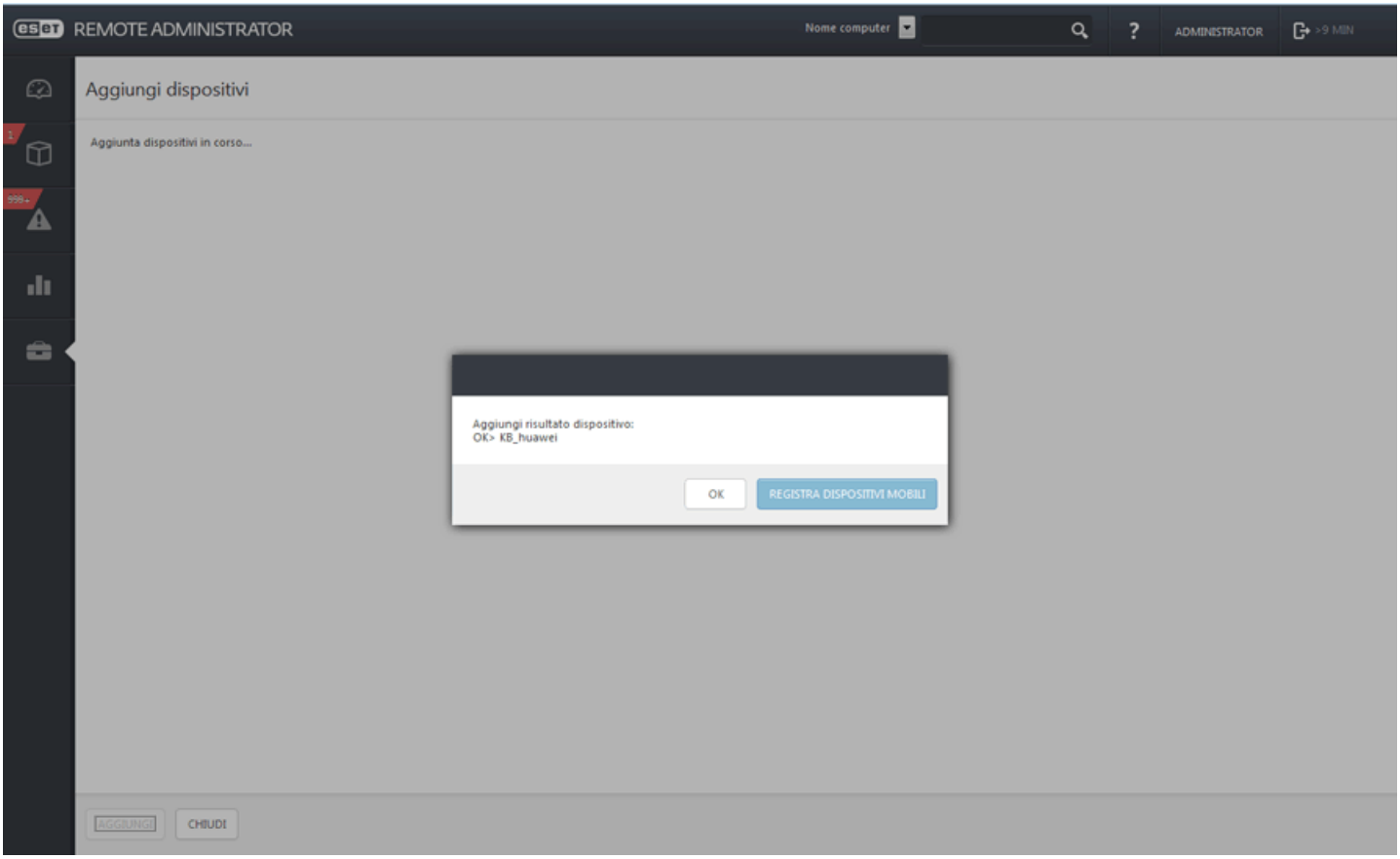
4.5.4 Registrazione dispositivo mobile

È possibile aggiungere dispositivi mobili alla struttura ERA attenendosi alla stessa procedura utilizzata per aggiungere un nuovo computer. Per eseguire questa operazione, seguire i passaggi sottostanti:

1. Fare clic su **Amministrazione** > selezionare il gruppo statico al quale si desidera aggiungere il dispositivo mobile e fare clic su **Nuovo...**
2. Selezionare **Dispositivi mobili** e inserire un **Nome**, una **Descrizione**(facoltativa) e un **Numero di identificazione** del dispositivo. I numeri di identificazione dei dispositivi possono essere numeri IMEI (reti GSM), numeri MEID (reti CDMA) o indirizzi Wi-Fi MAC (solo per dispositivi mobili Wi-Fi).



3. Esistono due diversi modi per registrare un dispositivo mobile:
   a. L'amministratore può ottenere preventivamente l'indirizzo MAC dal dispositivo e registrare il dispositivo tramite ERA con il metodo tradizionale
   b. L'utente fa clic su un collegamento per la registrazione (inviato dall'amministratore). L'app risponderà automaticamente che il dispositivo non è inserito nella whitelist/approvato e sullo schermo verrà visualizzato l'indirizzo MAC. All'utente verrà quindi richiesto di contattare l'amministratore e fornire il numero di identificazione del dispositivo (ovvero, l'indirizzo MAC).
4. Fare clic su **Aggiungi**, quindi fare clic su **Registra dispositivi mobili** nella finestra di dialogo.



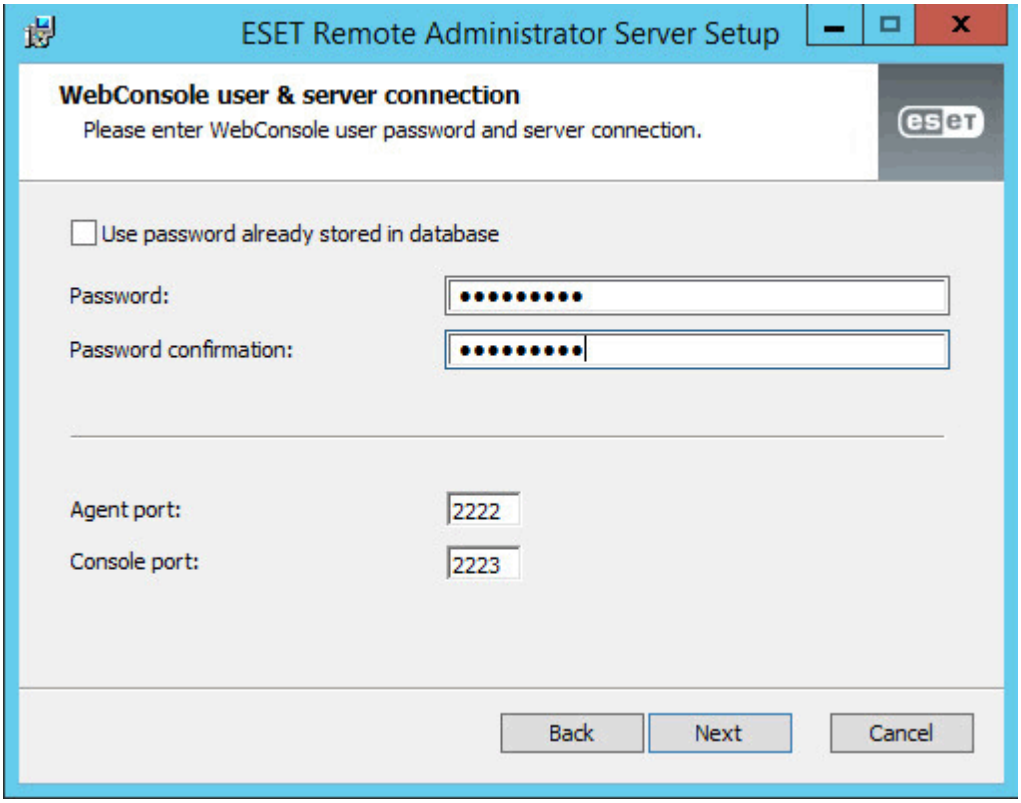
La procedura guidata dell'attività Registrazione dispositivo guiderà l'utente attraverso il processo di registrazione del dispositivo mobile.

4.6 Procedure consigliate

Password dimenticata: idealmente, l'account amministratore dovrebbe essere utilizzato esclusivamente per la creazione di account di singoli amministratori. Una volta creati, gli account di amministratore non devono essere utilizzati ed è necessario salvarne la password. Questa procedura consente di utilizzare l'account di amministratore per la reimpostazione delle password o dei dettagli dell'account dei singoli amministratori, qualora necessario.

Come fare per **reimpostare la password** di un account ERA Administrator integrato:

- aprire **Programmi e funzioni** (eseguire appwiz.cpl), individuare ESET Remote Administrator Server e fare clic con il pulsante destro del mouse su di esso
- selezionare **Modifica** dal menu contestuale
- scegliere **Ripara**
- specificare i dettagli di connessione del database
- selezionare **Utilizza il database esistente** e applicare l'aggiornamento
- assicurarsi di deselezionare l'opzione **Utilizzare la password già archiviata nel database** e inserire una nuova password.
- a questo punto è possibile effettuare l'accesso a ERA Web Console con la nuova password



4.6.1 Gestione utenti

Si consiglia vivamente di creare account aggiuntivi con diritti di accesso specifici in base alle competenze desiderate.

5. Utilizzo di ESET Remote Administrator

I client vengono gestiti attraverso **ERA Console Web**. alla quale è possibile accedere da qualsiasi dispositivo mediante un browser compatibile. La console Web è suddivisa in tre sezioni principali:

1. Nella parte superiore della console Web, è possibile utilizzare lo strumento di **Ricerca rapida**. Digitare il **Nome del client** o l' **Indirizzo IPv4/IPv6** e fare clic sul simbolo della lente di ingrandimento oppure premere **Invio**. L'utente verrà reindirizzato alla sezione Gruppi, dove sarà possibile visualizzare i client corrispondenti.

2. Il menu sulla sinistra contiene le sezioni principali di ESET Remote Administrator e i seguenti Collegamenti rapidi:

- Dashboard
- Computer
- Minacce
- Report
- Amministrazione

Collegamenti rapidi

- Nuovo utente nativo
- Nuovo criterio
- Nuova attività client
- Programmi di installazione live dell'agente

3. I pulsanti nella parte inferiore della pagina sono unici per ciascuna sezione e funzione e sono descritti in modo dettagliato nei capitoli corrispondenti.

NOTA: Il pulsante di colore rosso **Impostazioni obbligatorie**, comune a tutti i nuovi elementi, viene visualizzato nel caso in cui le impostazioni obbligatorie non sono state configurate e, di conseguenza, non è possibile proseguire con la creazione. Tale condizione è inoltre indicata dalla presenza di un punto esclamativo rosso accanto a ciascuna sezione. Fare clic su **Impostazioni obbligatorie** per accedere alla sezione in cui sono posizionate le impostazioni in questione.

Regole generali

- Le impostazioni richieste (obbligatorie) sono sempre contrassegnate con un punto esclamativo rosso accanto alla sezione e ai valori corrispondenti. Per accedere alle impostazioni obbligatorie (se applicabile), fare clic su **Impostazioni obbligatorie** nella parte inferiore di ciascuna pagina.
- Se si desidera ricevere assistenza relativamente all'utilizzo di ESET Remote Administrator, fare clic sull'icona **?** nell'angolo in alto a destra oppure scorrere fino in basso nel riquadro sulla sinistra e fare clic su **Guida**. Verrà visualizzata la finestra della guida corrispondente delle pagina corrente.
- La sezione **Amministrazione** è riservata a specifiche configurazioni. Per ulteriori informazioni, leggere il capitolo Amministrazione.

5.1 Dashboard

Quella del dashboard è la pagina predefinita che viene visualizzata dopo il primo accesso dell'utente a ERA Web Console. In essa vengono visualizzati i report predefiniti sulla rete. È possibile passare da un dashboard all'altro utilizzando le schede nella barra dei menu in alto. Ciascun dashboard comprende vari report. È possibile personalizzare i dashboard aggiungendo report, modificando quelli esistenti, ridimensionandoli, spostandoli e riordinandoli. Tutte queste funzioni offrono all'utente una panoramica completa di ESET Remote Administrator e dei suoi componenti (client, gruppi, attività, criteri, utenti, competenze, ecc.). ESET Remote Administrator presenta quattro dashboard predefiniti:

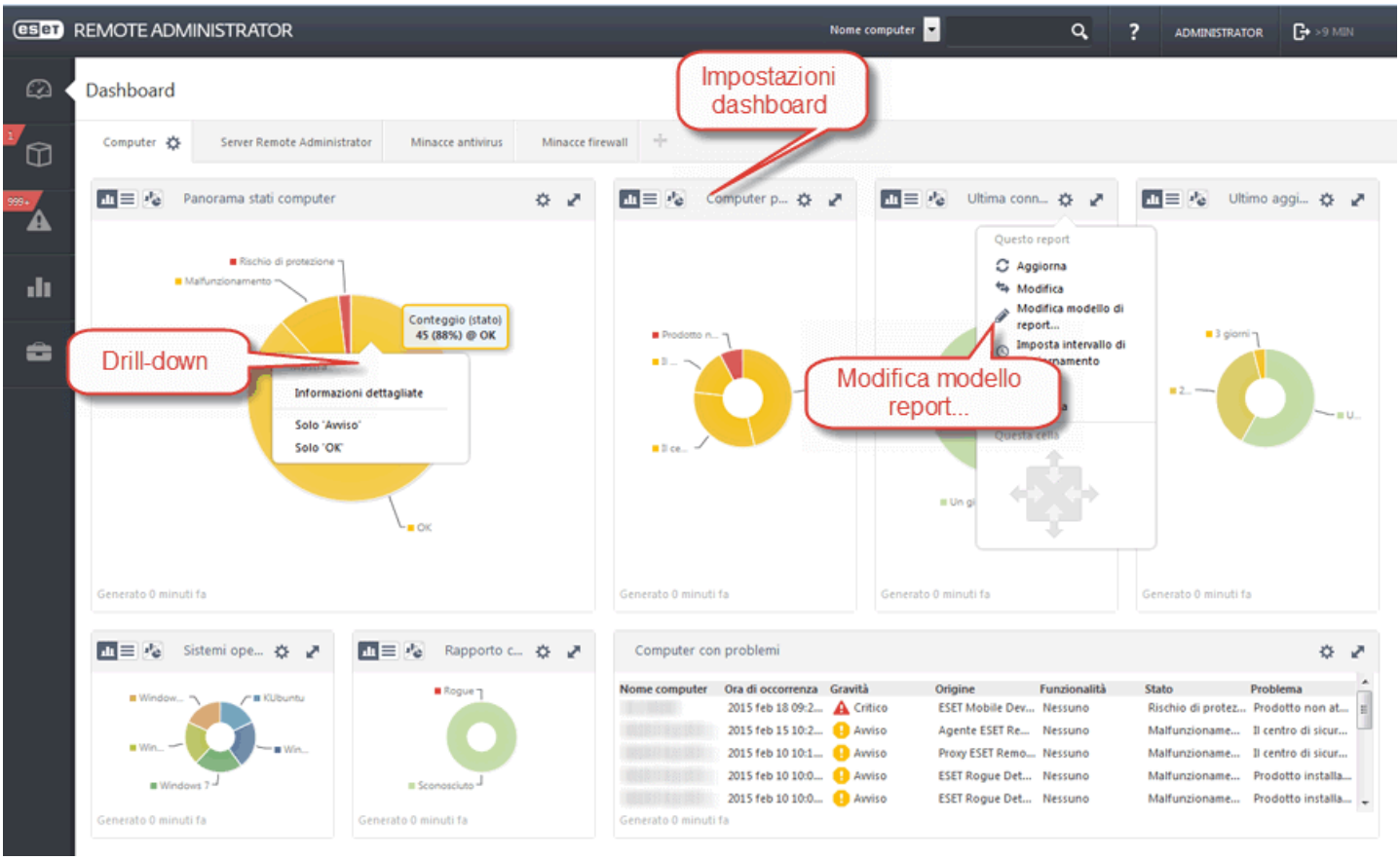
Computer
Questo dashboard offre all'utente una panoramica delle macchine client: lo stato di protezione, i sistemi operativi, lo stato degli aggiornamenti, ecc.

Server Remote Administrator
In questo dashboard, è possibile visualizzare informazioni relative al server ESET Remote Administrator stesso: il carico, i client con problemi, il carico di CPU, le connessioni del database, ecc.

Minacce antivirus
In questa sezione è possibile visualizzare i report dal modulo antivirus dei prodotti di protezione client: minacce attive, minacce degli ultimi 7/30 giorni e così via.

Minacce firewall
Eventi firewall dei client collegati in base al livello di gravità, all'ora della segnalazione, ecc.

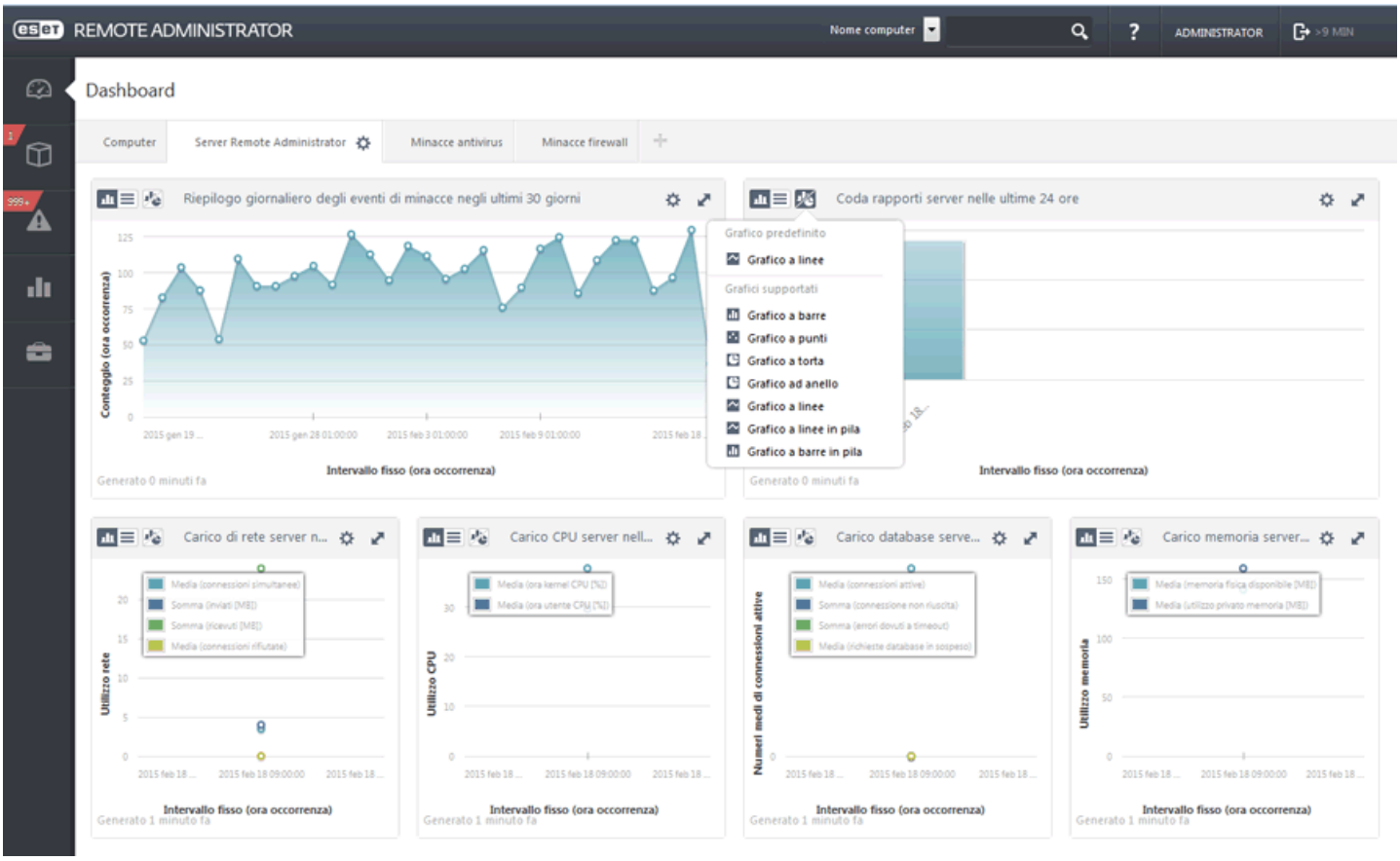
Funzionalità dashboard:



5.1.1 Impostazioni dashboard

Le impostazioni del dashboard, che sono disponibili sia per quelli predefiniti sia per quelli di nuova creazione, consentono all'utente di gestire questa risorsa. Le opzioni disponibili sono illustrate di seguito:

- **Aggiungi un nuovo dashboard**: fare clic sul simbolo + sopra all'intestazione del dashboard. Inserire un nome per il nuovo dashboard e fare clic su **OK** per confermare. Verrà creato un nuovo dashboard con un campo Report vuoto. Dopo aver configurato il dashboard, è possibile iniziare ad aggiungere i report.
- **Duplica dashboard**: selezionare il dashboard che si desidera duplicare e fare clic sul simbolo della **rotella** accanto al nome del dashboard. Selezionare **Duplica** dall'elenco per creare un dashboard duplicato.
- **Sposta dashboard**: fare clic e trascinare il nome di un dashboard per modificarne la posizione rispetto ad altri dashboard.
- **Modifica la dimensione del dashboard (numero di report visualizzati)**: fare clic sul simbolo a forma di **rotella** > **Modifica layout**. Selezionare il numero di report che si desidera visualizzare nel dashboard (trascinare) e fare clic sui vari elementi. Il layout del dashboard verrà modificato.
- **Rinomina un dashboard**: fare clic sul simbolo a forma di **rotella** accanto al nome del dashboard e su **Rinomina**. Inserire un nuovo nome per il dashboard e fare clic su **OK**.
- **Rimuovi un dashboard**: fare clic sul simbolo a forma di **rotella** accanto al nome del dashboard, quindi su **Rimuovi** e confermare la rimozione.
- **Ridimensiona**: fare clic sul simbolo della **doppia freccia** sulla destra del report da ridimensionare. I report più rilevanti presentano dimensioni maggiori rispetto a quelli meno rilevanti. È inoltre possibile visualizzare i report in modalità schermo intero.



- **Modifica tipo di grafico**: fare clic sul simbolo del **Grafico** nell'angolo in alto a sinistra e passare a **Grafico a torta**, **Grafico a linee** ecc. per cambiare il tipo di grafico.
- Fare clic su **Aggiorna** per aggiornare le informazioni visualizzate.
- Fare clic su **Modifica** per visualizzare un report differente.
- Fare clic su Modifica modello di report per aggiungere e modificare un modello.
- Fare clic su **Imposta intervallo di aggiornamento** per definire la frequenza di aggiornamento dei dati del report. **L'intervallo di aggiornamento predefinito è 120 secondi**.
- **Rinomina/Rimuovi**: consente di rinominare/rimuovere il report.

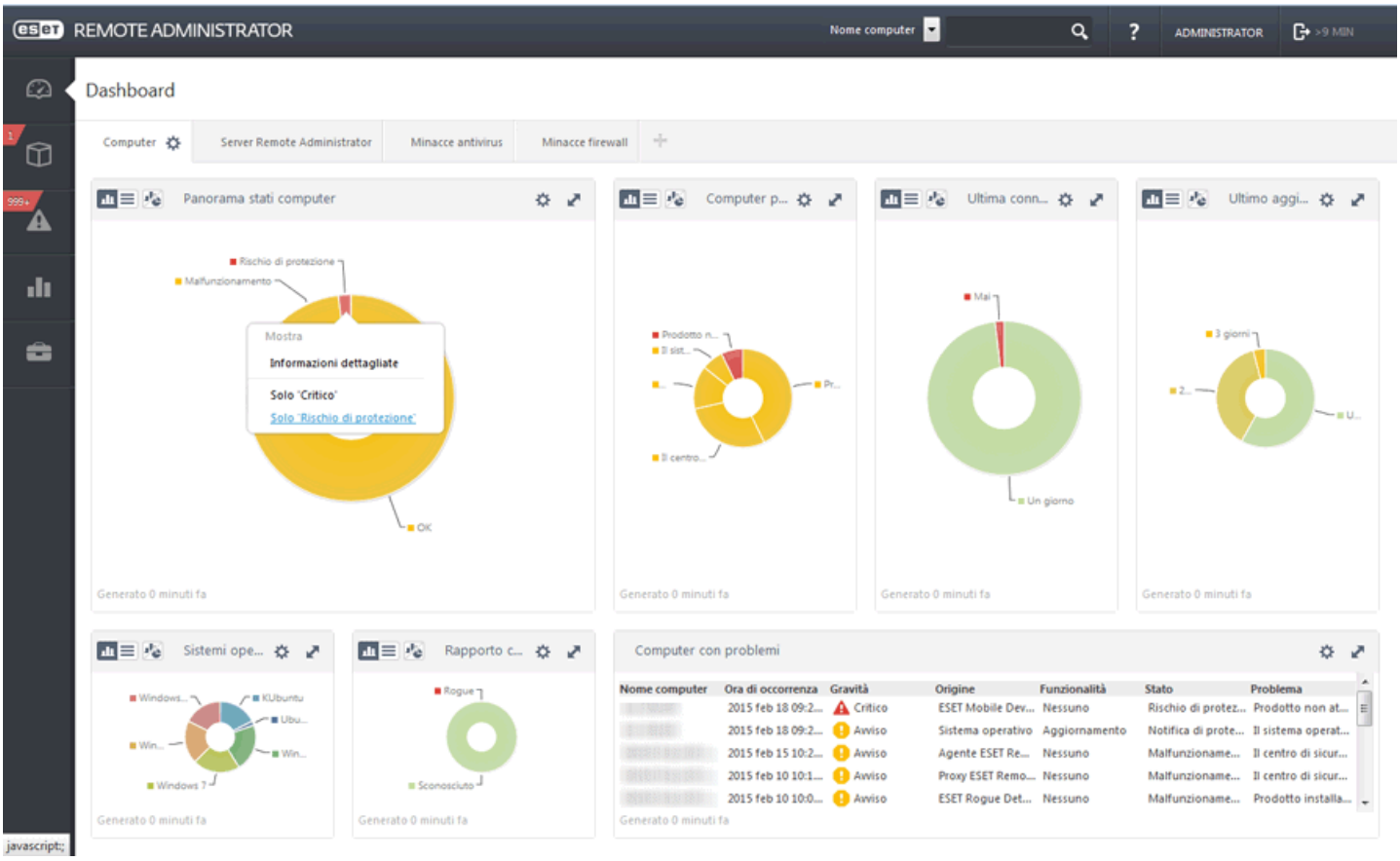
5.1.2 Drill down

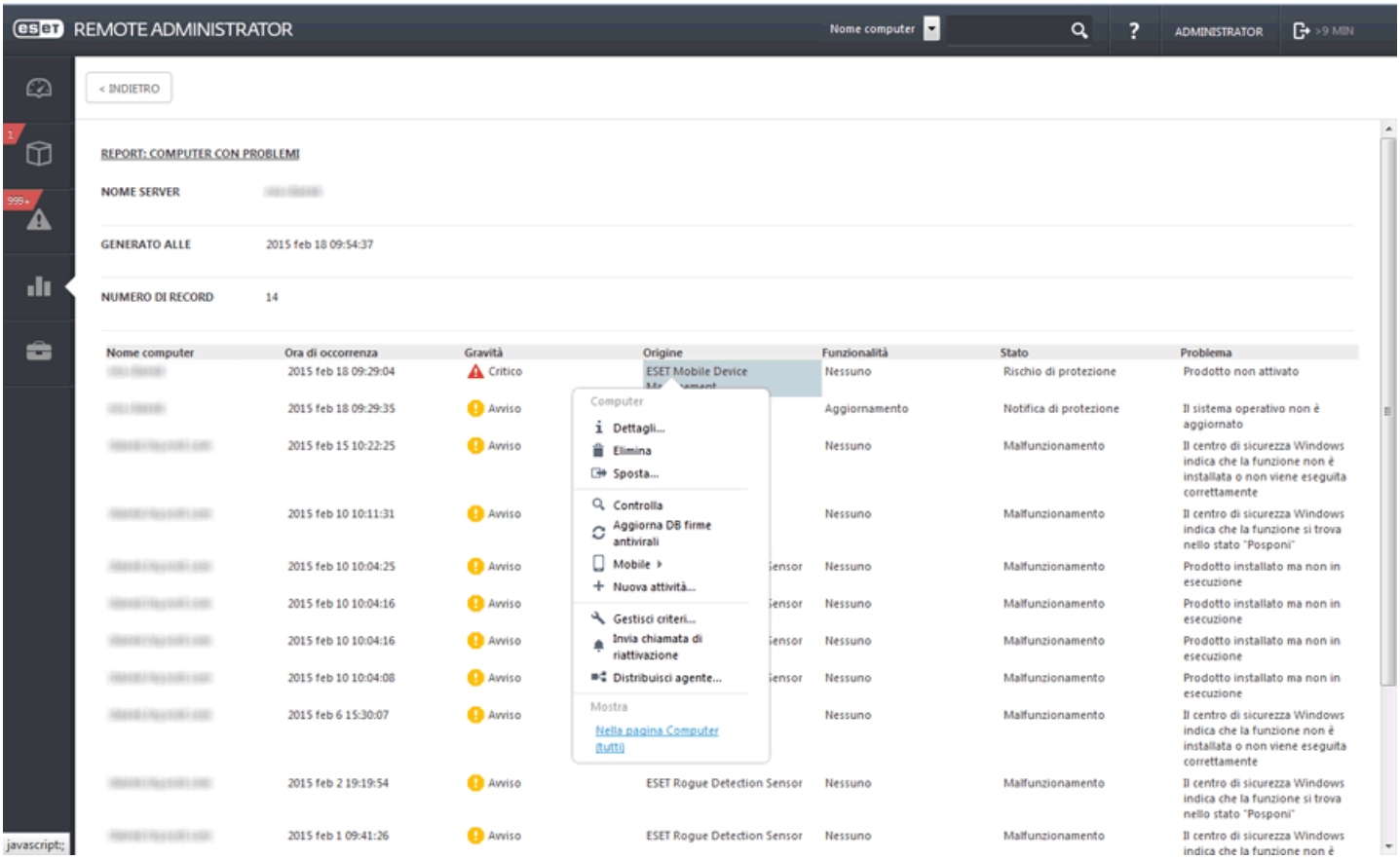
Il dashboard è una funzionalità utile per condurre un'analisi approfondita dei dati. Consente di selezionare in modo interattivo un elemento specifico da un riepilogo e di visualizzarne le informazioni dettagliate. La procedura si basa sul recupero di informazioni approfondite su uno specifico elemento da un riepilogo. Il recupero dei dati viene solitamente condotto su più livelli.

Esistono quattro tipi di drill down:

- Mostra **Informazioni dettagliate**: nome e descrizione del computer, nome del Gruppo statico, ecc. Consente di visualizzare i dati originali (non aggregati) relativi alla riga selezionata.
- Mostra **Solo '***value***'**: informazioni, critiche, rischio per la protezione, notifica di sicurezza, ecc.
- **Espandi colonna '***value***'**: consente di visualizzare le informazioni aggregate (generalmente per il conteggio o la somma). Ad esempio, se nella colonna è presente solo un numero e si seleziona **Espandi colonna Computer**, verranno visualizzati tutti i dettagli sui computer
- Mostra **Nella pagina Computer (tutti)**: reindirizza l'utente alla pagina Computer (viene visualizzato solo il risultato di 100 elementi)

NOTA: la funzione di drill down degli altri report consente di visualizzare soltanto i primi 1000 elementi.

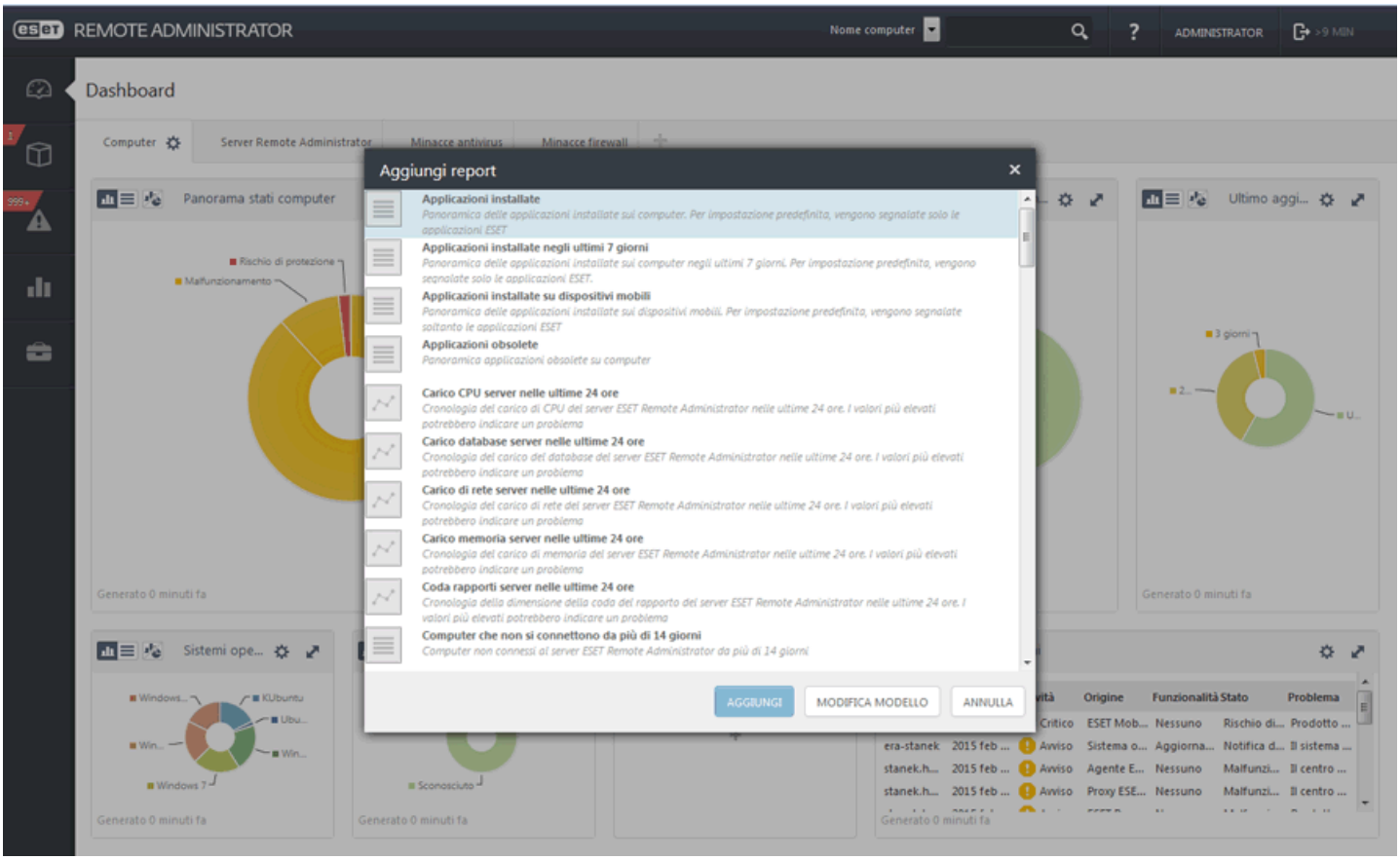




5.1.3 Modifica modello di report

In questa sezione vengono illustrate le modalità di modifica dei modelli di report esistenti (per ulteriori informazioni sulle modalità di creazione di un nuovo modello di report, fare clic qui).

Fare clic su un **riquadro vuoto** visualizzato nel nuovo dashboard. Verrà visualizzata la finestra Aggiungi report. Selezionare Applicazioni installate e fare clic su **Aggiungi** o Modifica modello.

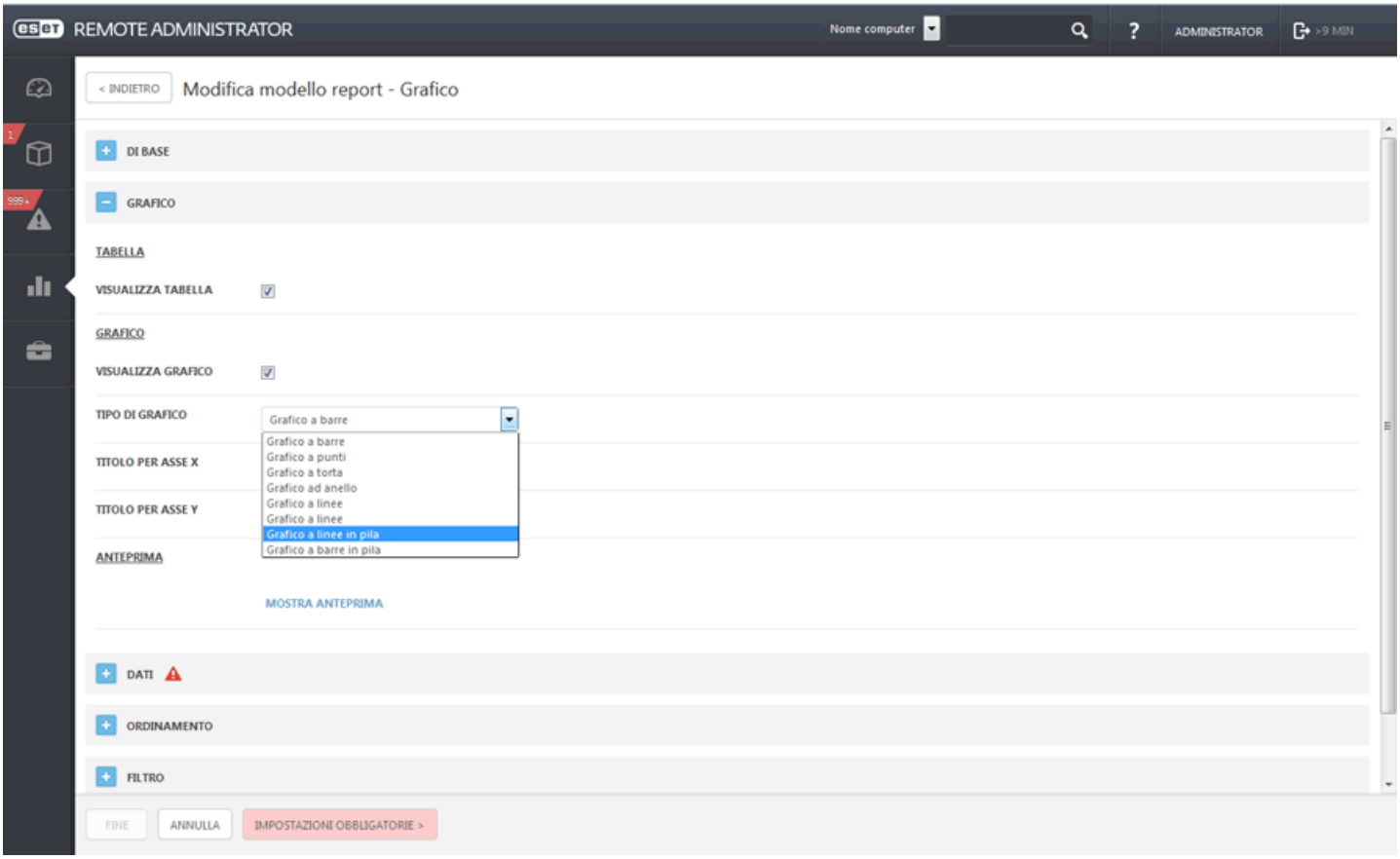


Di base

Modificare le informazioni **di base** sul modello. Rivedere o modificare il **Nome**, la **Descrizione** e una **Categoria**. Queste informazioni sono predefinite in base al tipo di **Report** selezionato.

Grafico

Nella sezione **Grafico**, selezionare il tipo di **Report**. In questo esempio, l'opzione **Visualizza tabella** è stata lasciata vuota ed è stata selezionata l'opzione **Visualizza grafico**.

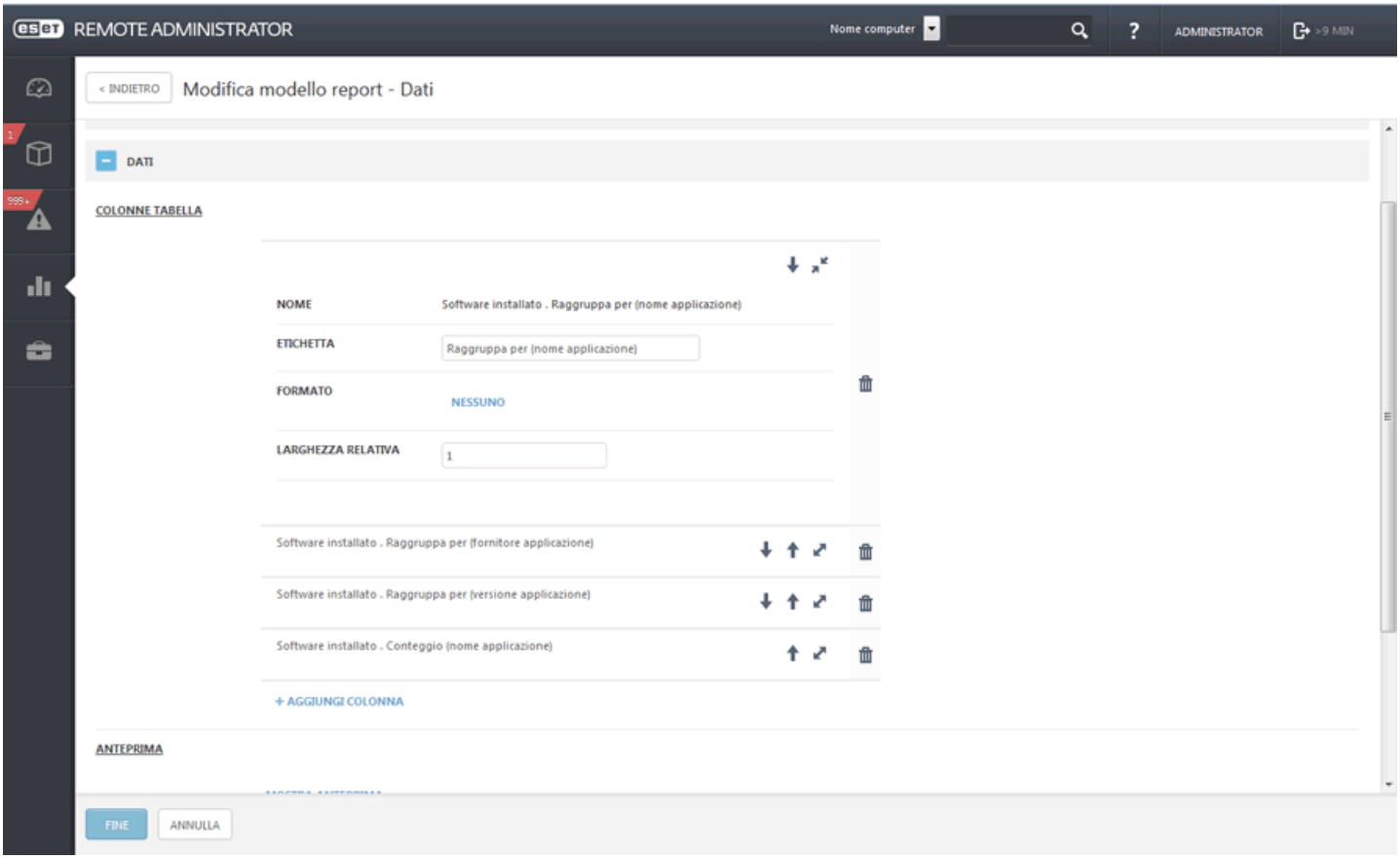


NOTA: ogni tipo di grafico selezionato verrà visualizzato nella sezione **Anteprima**. In tal modo, sarà possibile visualizzare in tempo reale l'aspetto assunto dal report.

La selezione di un **Grafico** consente all'utente di utilizzare varie opzioni. Per avere un quadro più chiaro, è stato selezionato il **Tipo di grafico a linee in pila**. Questo tipo di grafico viene utilizzato se si desidera analizzare i dati con unità di misura diverse.

Facoltativamente, è possibile definire un titolo per l'asse **X** e per l'asse **Y** del grafico per renderne più agevoli la lettura e il riconoscimento delle tendenze.

Dati

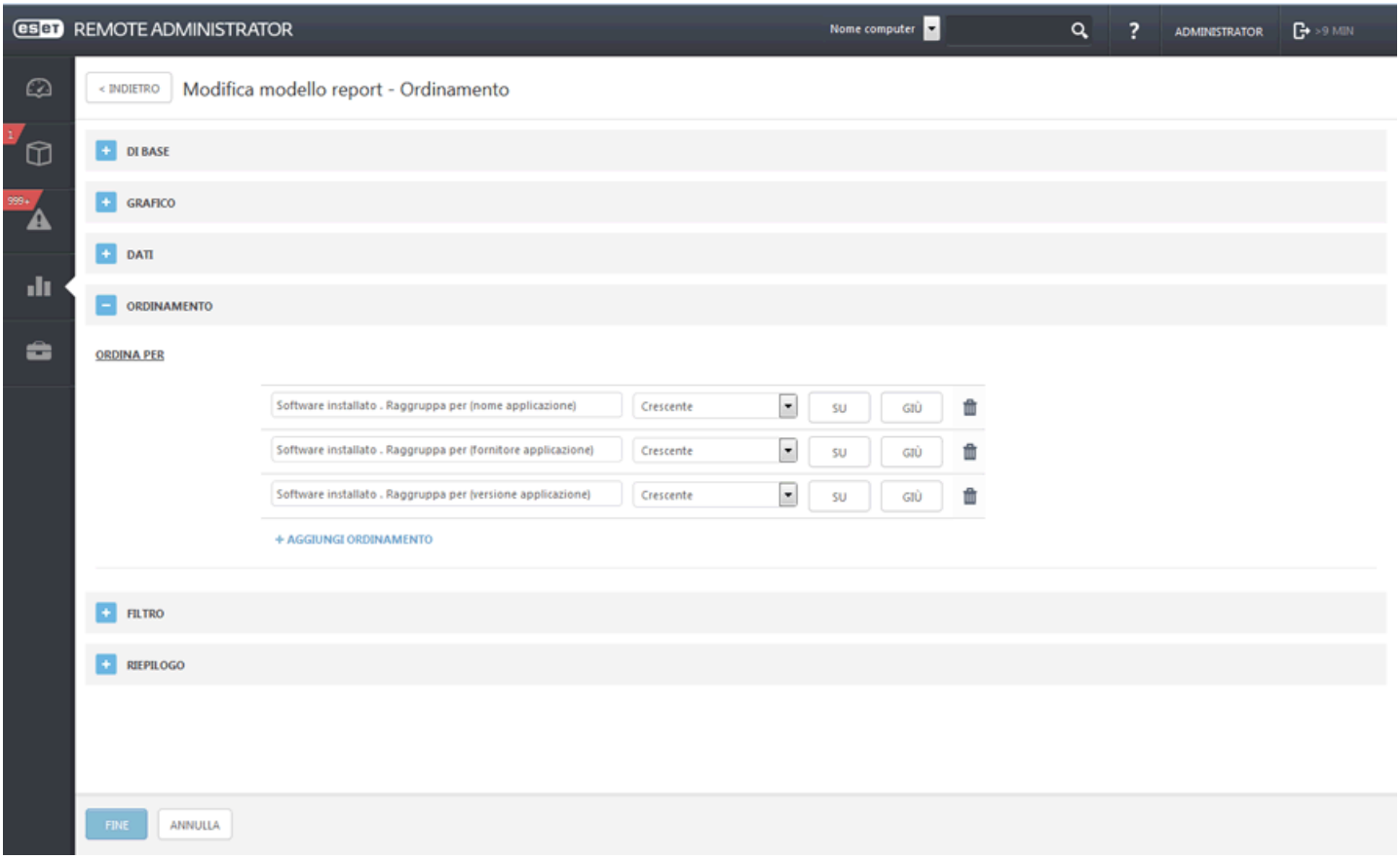


Nella sezione **Dati**, sono state inserite le informazioni da visualizzare sull'asse **X** e sull'asse **Y** del grafico. Facendo clic sui rispettivi simboli, si aprirà una finestra contenente le varie opzioni. Le scelte disponibili per l'asse **Y** dipendono sempre dalle informazioni selezionate per l'asse **X** e viceversa, in quanto sul grafico viene visualizzata la relazione tra questi due elementi. È necessario, inoltre, che i dati siano compatibili.

Per l'asse **X**, è stato selezionato **Computer** > **Nome computer** per individuare i computer che inviano spam. Il **Formato** verrà impostato su **Valore** > **Assoluto**. Il colore e le icone sono impostati dall'amministratore.

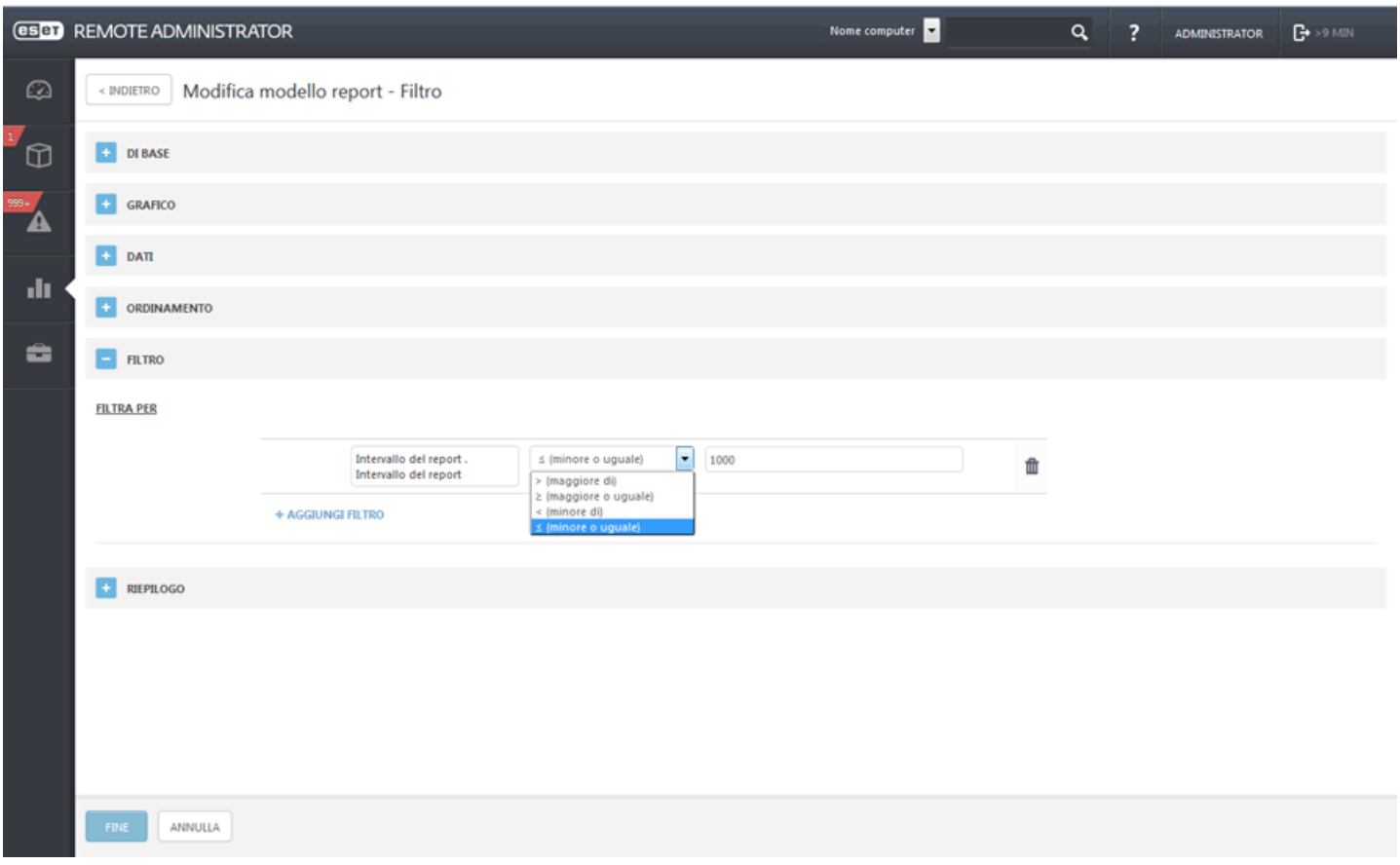
Per l'asse **Y**, selezionare **Software installato** > **Dimensioni in MB** per determinare il numero assoluto dei messaggi spam. Il **Formato** verrà impostato su **Valore** > **Assoluto**. Il colore e le icone sono impostati dall'amministratore.

Ordinamento



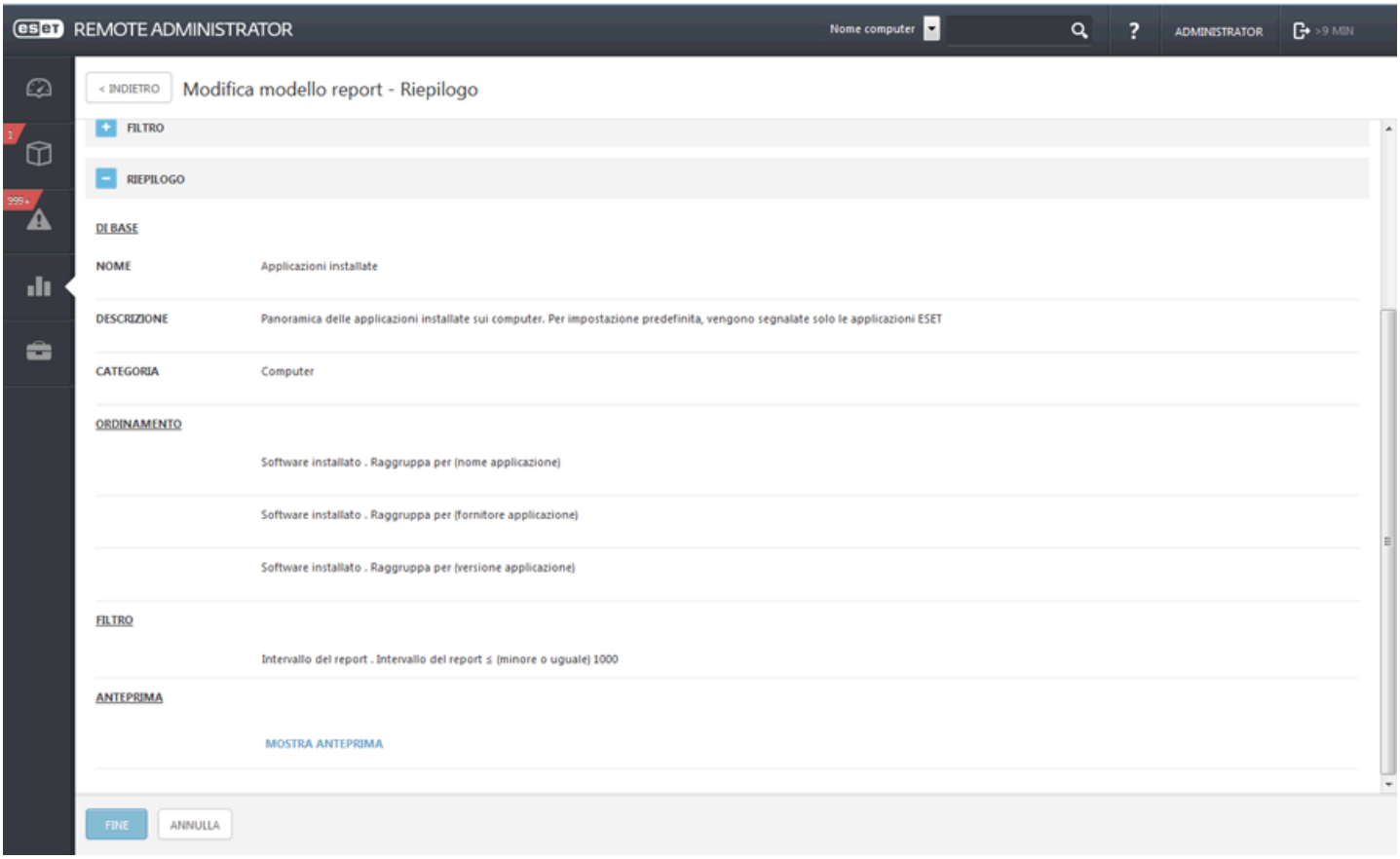
Aggiungi ordinamento: consente di definire la relazione tra i dati selezionati. Selezionare le informazioni di partenza e il metodo di ordinamento tra **Crescente** e **Decrescente**. È inoltre possibile ordinare i dati utilizzando entrambe le opzioni (visualizzate in precedenza).

Filtro



Le opzioni visualizzate qui dipendono dalle impostazioni configurate in precedenza (informazioni per l'asse X e per l'asse Y). Selezionare un'opzione e una funzione matematica per determinare il metodo di filtraggio dei dati. Per questo esempio, è stato selezionato **Software installato** e **Nome dell'applicazione** > **è uguale a** > **ESS** e **Software installato**. **Dimensione in MB** > **è maggiore di** > **50**.

Riepilogo



Nel **Riepilogo**, rivedere le opzioni e le informazioni selezionate. Se il valore è corretto, fare clic su **Fine** per creare un **Modello di report**.

5.2 Computer

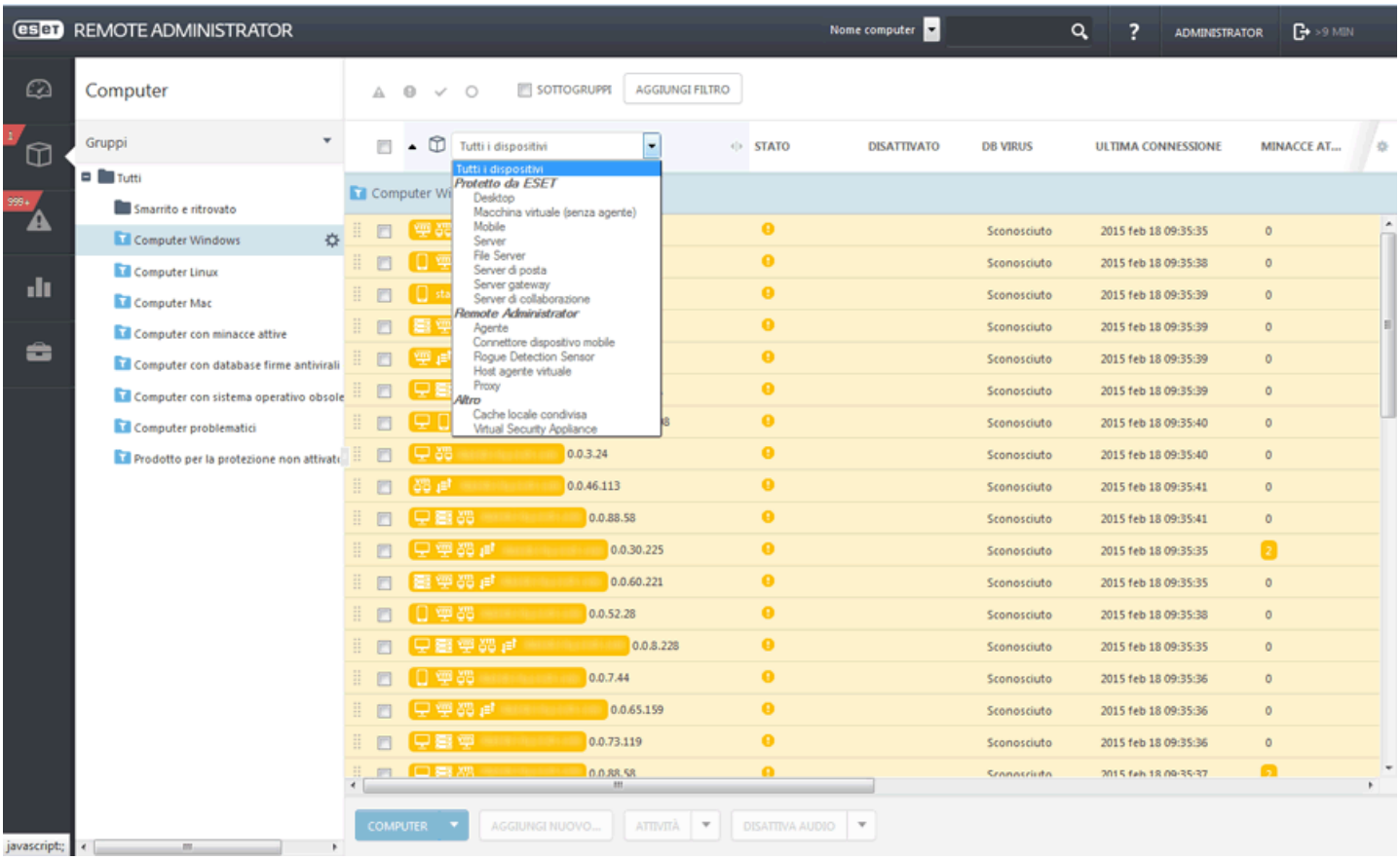
Tutti i computer client aggiunti a ESET Remote Administrator vengono visualizzati qui e sono suddivisi in Gruppi. Facendo clic su un gruppo dell'elenco (sulla sinistra), è possibile visualizzare i relativi membri (client) nel riquadro sulla destra. È possibile filtrare i client utilizzando i filtri nella parte superiore della pagina; facendo clic su **Aggiungi filtro**, sarà possibile visualizzare i criteri di filtraggio. Sono inoltre disponibili alcuni filtri predefiniti a cui è possibile accedere rapidamente:

- Quattro icone che consentono all'utente di filtrare i valori in base al livello di gravità (rosso: **Errori**, giallo: **Avvisi**, verde: **Comunicazioni** e grigio: Computer **non gestiti**). L'icona della gravità rappresenta lo stato corrente del prodotto ESET su uno specifico computer client. È possibile utilizzare una combinazione di queste icone attivandole o disattivandole. Ad esempio, per visualizzare solo i computer contenenti avvisi, lasciare attivata solo l'icona gialla (il resto delle icone deve essere disattivato). Per visualizzare sia gli avvisi che gli errori, lasciare attive solo queste due icone.
- Casella di controllo **Sottogruppi**: consente di visualizzare i sottogruppi del gruppo attualmente selezionato.
- I computer **non gestiti** (client sulla rete privi dell'agente ERA o di un prodotto di protezione ESET installato) compaiono solitamente nel gruppo **Smarrito e trovato**.

L'utilizzo del menu a discesa sotto ai filtri consente di limitare i client visualizzati (computer). Sono disponibili alcune categorie:

- Selezionare **Tutti i dispositivi** dal menu a discesa per visualizzare nuovamente tutti i computer client senza limitare (filtrare) i client visualizzati. Per la riduzione della visualizzazione, è possibile utilizzare una combinazione di tutte le opzioni di filtraggio indicate in precedenza.
- **Protetto da ESET** (protetto da un prodotto ESET)
- **Amministratore remoto** (singoli componenti ERA quali Agente, RD Sensor, Proxy e così via)
- **Altro** (Cache locale condivisa, Accessori virtuali). Dopo aver effettuato la selezione, verranno visualizzati solo i rispettivi client.

NOTA: qualora non si riesca a trovare uno specifico computer nell'elenco e si sia sicuri del fatto che esso è presente nell'infrastruttura ERA, assicurarsi che tutti i filtri siano disattivati.



È possibile utilizzare il menu contestuale (icona a forma di rotella ⚙) per creare un gruppo statico o dinamico, creare una nuova attività o selezionarne una tra le altre azioni disponibili.

Azioni pulsante **Computer**:

+ Nuovo...
Aggiungi manualmente dispositivi non trovati o aggiunti automaticamente.

Dettagli...
- **Di base** (Nome, Gruppo padre, Dispositivo, Informazioni sul sistema operativo, ecc.)
- **Configurazione** (Configurazione, Criteri applicati, ecc.)
- **Esecuzioni attività** (Verificata, Nome attività, Tipo di attività, Stato, ecc.)
- **Applicazioni installate** (Nome, Fornitore, Versione, L'agente supporta la disinstallazione, ecc.)
- **Avvisi** (Problema, Stato, ecc.)
- **Minacce** (Tutti i tipi di minacce, Disattivata, Causa, ecc.)
- **Quarantena** (Nome minaccia, Tipo minaccia, Nome oggetto, Hash, ecc.)

Elimina
Tale operazione rimuoverà il client dall'elenco. Tuttavia, finché rimarrà nella rete, comparirà nel gruppo Smarrito e trovato.

Sposta...
È possibile spostare il client in un altro gruppo. La selezione di questa opzione consente di visualizzare un elenco di gruppi disponibili.

Gestisci criteri...
È inoltre possibile assegnare un Criterio direttamente a un client (client multipli) e non solo a un gruppo. Selezionare questa opzione per assegnare il criterio al/i client selezionato/i.

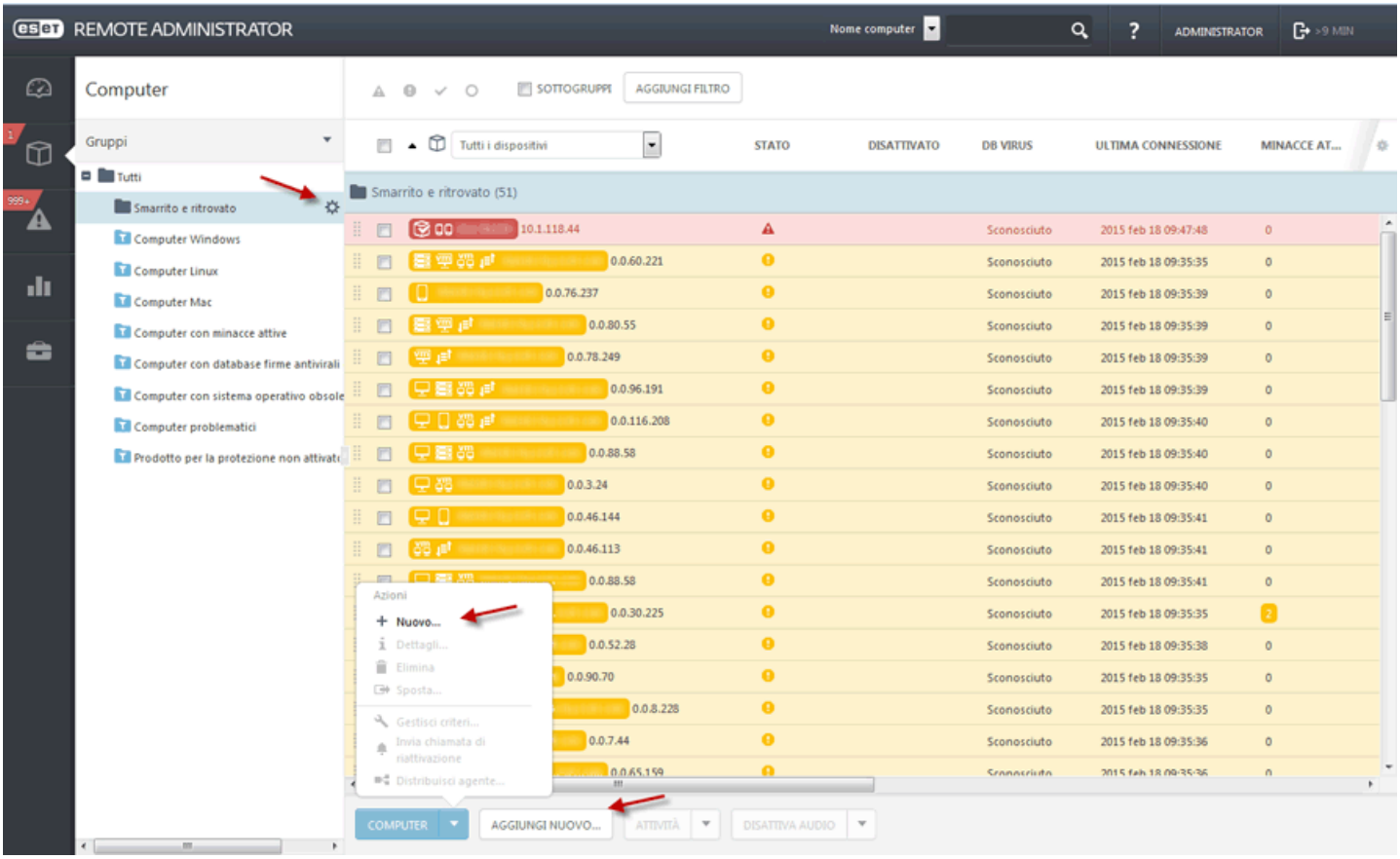
Invia chiamata di riattivazione
Il server ERA avvia una comunicazione immediata con l'agente ERA su una macchina client. Questa opzione è utile se non si desidera attendere l'intervallo periodico in cui l'agente ERA si connette al server ERA. Ciò vale, ad esempio, se si desidera eseguire immediatamente un'Attività client sui client oppure applicare subito un Criterio.

NOTA: se si apporta una modifica e si desidera applicarla, attendere all'incirca un minuto prima di utilizzare la chiamata di riattivazione.

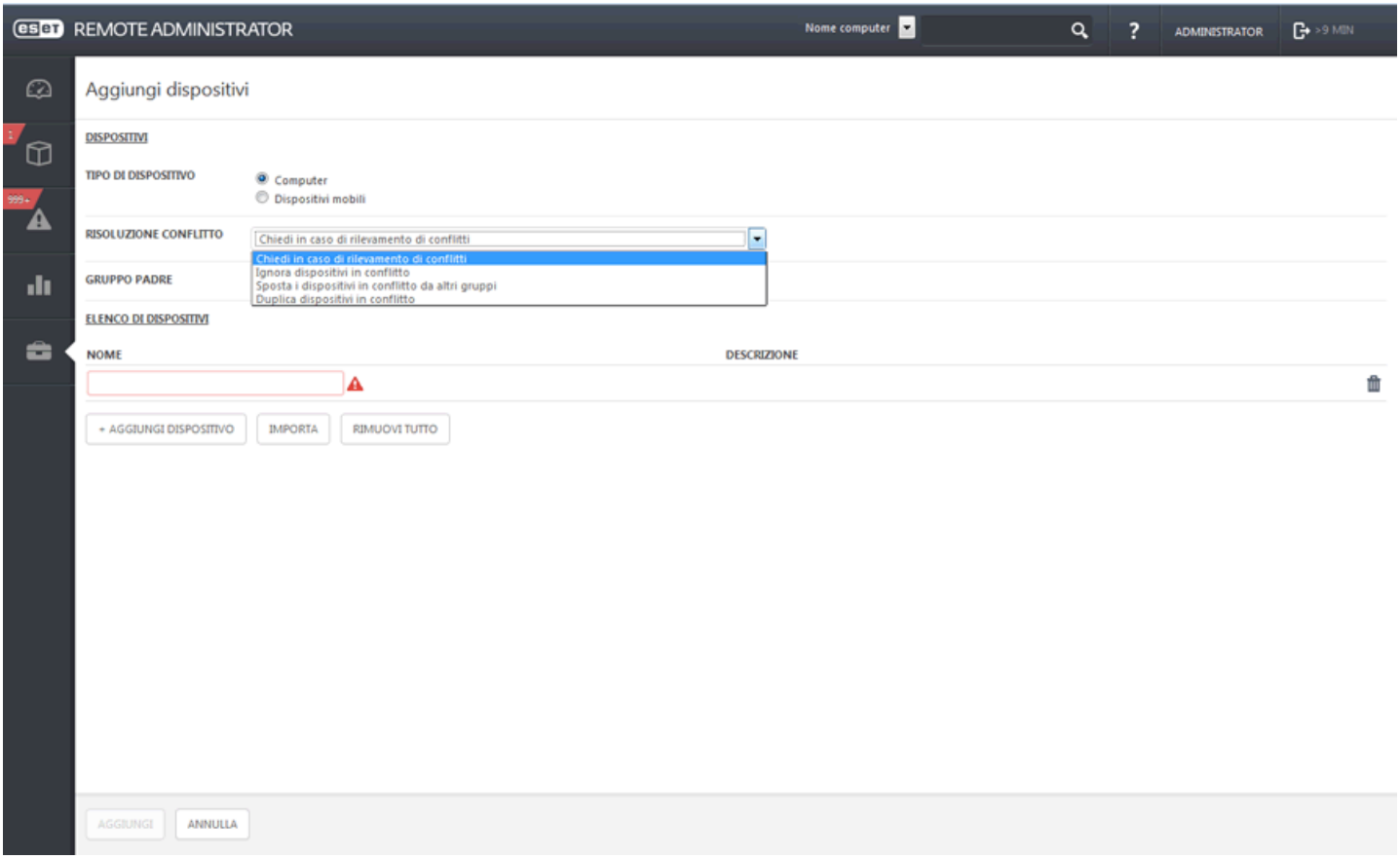
Distribuisci agente...
Questa opzione consente all'utente di creare una nuova attività server.

5.2.1 Aggiungi computer

Nella **scheda** Computer è possibile aggiungere nuovi computer in base a tre diverse modalità. Ad esempio, selezionare un gruppo statico: fare clic sull'icona a forma di rotella e selezionare **+ Aggiungi nuovo**.



Immettere il nome del computer che si desidera aggiungere nel campo **Nome**. Fare clic su + Aggiungi dispositivo per aggiungere altri computer oppure su Importa per importare un file contenente un elenco di computer da aggiungere. Facoltativamente, inserire una **descrizione** dei computer.



Utilizzare il menu a discesa Risoluzione conflitto per selezionare l'azione da eseguire se un computer che si sta aggiungendo esiste già in ERA:

Chiedi in caso di rilevamento di conflitti: in caso di rilevamento di un conflitto, il programma chiederà all'utente di selezionare un'azione (vedere le opzioni sottostanti).
Ignora computer in conflitto: I computer duplicati non verranno aggiunti.
Sposta i computer in conflitto da altri gruppi: i computer in conflitto verranno spostati dai gruppi originali al gruppo **Tutti**.
Duplica computer in conflitto: verranno aggiunti nuovi computer, ma con nomi diversi.

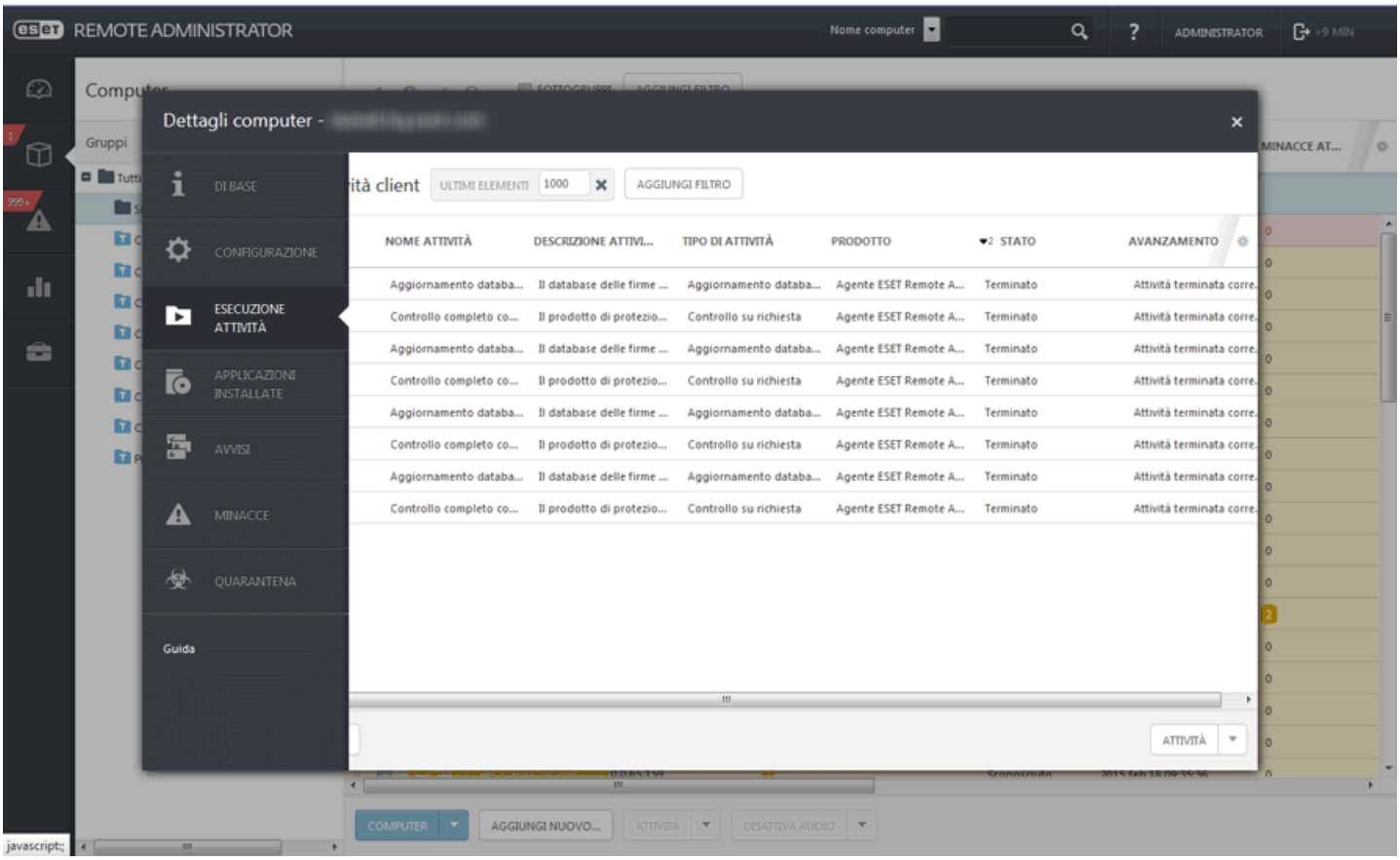
Fare clic su **Aggiungi**. È possibile visualizzare i computer nell'elenco sulla destra dopo aver selezionato il relativo gruppo di appartenenza.

NOTA: l'aggiunta di computer multipli potrebbe richiedere più tempo. Potrebbe essere eseguita una ricerca DNS inversa.

Per ulteriori informazioni sulle modalità di aggiunta dei dispositivi mobili, consultare il capitolo Registrazione dispositivi mobili.

5.2.2 Dettagli computer

Selezionare un computer nel Gruppo statico o dinamico e fare clic su **Dettagli** per visualizzare ulteriori informazioni su tale computer.



Il menu Dettagli computer contiene le seguenti impostazioni:

- **Di base**: è possibile modificare il nome, la descrizione e il gruppo padre del computer.
- **Configurazione:** consente di visualizzare l'intera configurazione, la connessione e i criteri applicati per questo computer.
- **Esecuzioni attività:** Verificata, Nome attività Tipo di attività, Stato
- **Applicazioni installate:** Nome, Versione, Dimensione, L'agente supporta la disinstallazione
- **Avvisi** : Problema, Stato, ecc.
- **Minacce:** Tutti i tipi di minacce, Disattivata, Causa, ecc.
- **Quarantena:** Nome minaccia, Tipo, Nome oggetto, Hash, ecc.

Attività azioni pulsante

Dopo aver selezionato uno o più computer e aver fatto clic su Attività, saranno disponibili le seguenti opzioni:

Controlla
L'utilizzo di questa opzione consentirà di eseguire l'attività Controllo su richiesta sul client che ha segnalato la minaccia.

Aggiorna DB firme antivirali
L'utilizzo di questa opzione consentirà di eseguire l'attività Aggiornamento del database delle firme antivirali (attiva manualmente un aggiornamento).

Mobile

- **Registra...** : questa opzione consente all'utente di creare una nuova attività client.
- **Trova** : opzione che consente di richiedere le coordinate GPS del dispositivo mobile.
- **Blocca**: il dispositivo verrà bloccato in caso di rilevamento di un'attività sospetta oppure nel caso in cui sia contrassegnato come mancante.
- **Sblocca** : il dispositivo verrà sbloccato.
- **Sirena** : attiva da remoto una sirena ad alto volume, anche se il dispositivo è in modalità silenziosa.
- **Cancella**: verranno cancellati definitivamente tutti i dati memorizzati sul dispositivo.

+ Nuova attività...

Selezionare un'attività e configurare la limitazione delle richieste (facoltativo). L'attività verrà accodata in base alle relative impostazioni.

Questa opzione attiva immediatamente un'attività esistente che l'utente seleziona da un elenco di attività disponibili. L'attivazione non è disponibile per questa attività, in quanto verrà eseguita immediatamente.

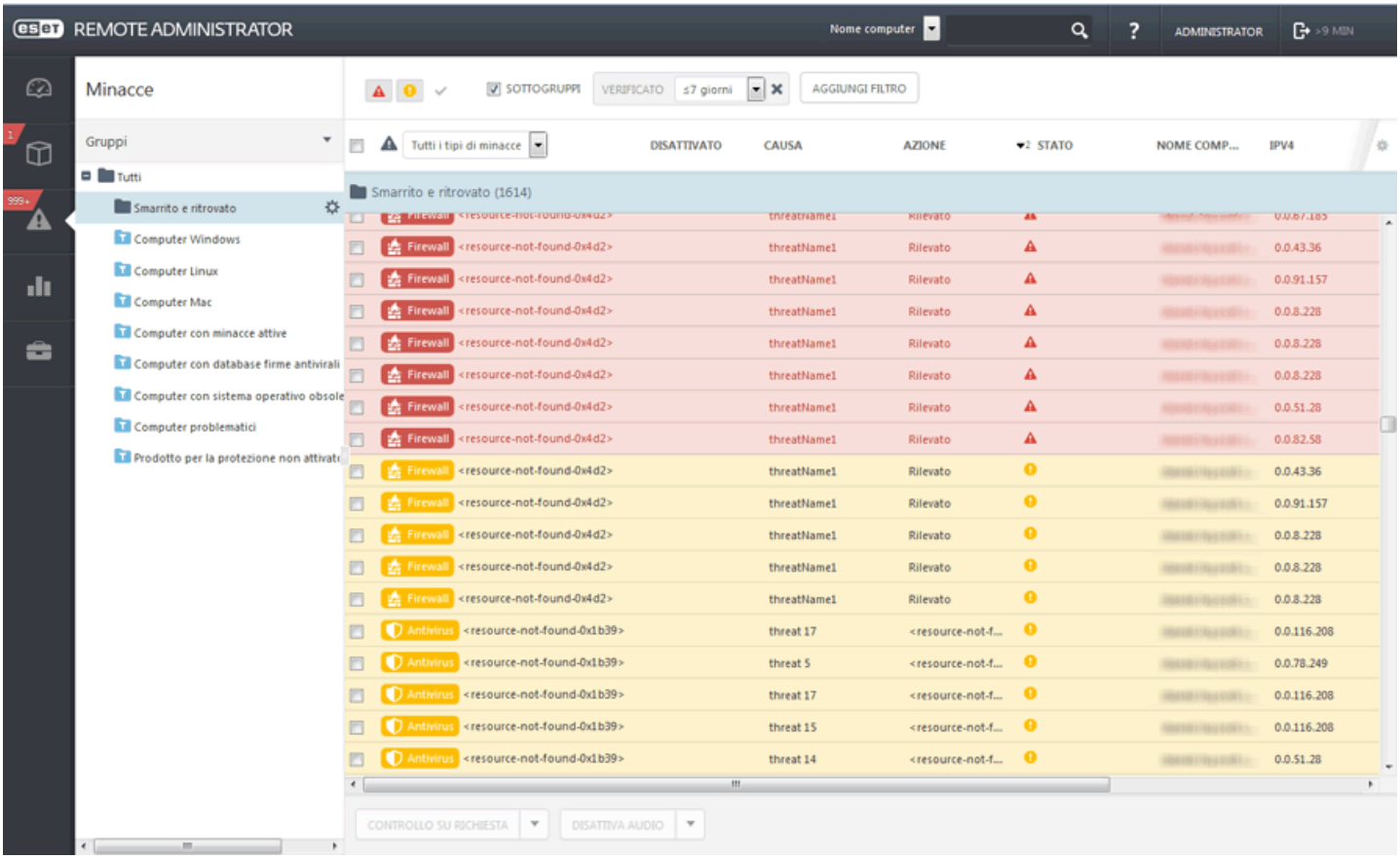
Disattiva

Dopo aver selezionato un computer e premuto su **Disattiva**, l'agente del client interromperà la segnalazione a ERA limitandosi ad aggregare le informazioni. Verrà visualizzata un'icona di disattivazione accanto al nome di un computer nella colonna Disattivazione.

Dopo aver disattivato l'opzione disattivazione facendo clic su **Disattiva** > **Riattiva**, il computer disattivato riprenderà nuovamente a inviare le segnalazioni e verrà ripristinata la comunicazione tra ERA e il client.

5.3 Minacce

La sezione **Minacce** offre all'utente una panoramica di tutte le minacce trovate sui computer presenti nella rete. Sul lato sinistro, viene visualizzata la struttura Gruppo. Da qui, è possibile sfogliare i gruppi e visualizzare le minacce sui membri di un dato gruppo. Selezionare il gruppo **Tutti** e utilizzare il filtro **Tutti i tipi di minacce** per visualizzare tutte le minacce trovate nei client di tutti i gruppi.



Filtro delle minacce

Le minacce possono essere filtrate utilizzando un filtro sopra l'elenco. Per impostazione predefinita, vengono visualizzati tutti i tipi di minacce degli ultimi 7 giorni. Per aggiungere più criteri di filtraggio, fare clic su **Aggiungi filtro** e selezionare un elemento dall'elenco: è possibile filtrare i risultati in base a **Nome** (nome della minaccia), **Causa** (causa della minaccia) o indirizzo **IPv4/IPv6** del client che ha segnalato la **Minaccia**.

Per impostazione predefinita, svengono visualizzati tutti i tipi di minaccia ma è possibile filtrare le minacce in base ad **Anti-virus** e **Firewall** per una visualizzazione più specifica.

Controllo su richiesta

L'utilizzo di questa opzione consentirà di eseguire l'attività Controllo su richiesta sul client che ha segnalato la minaccia.

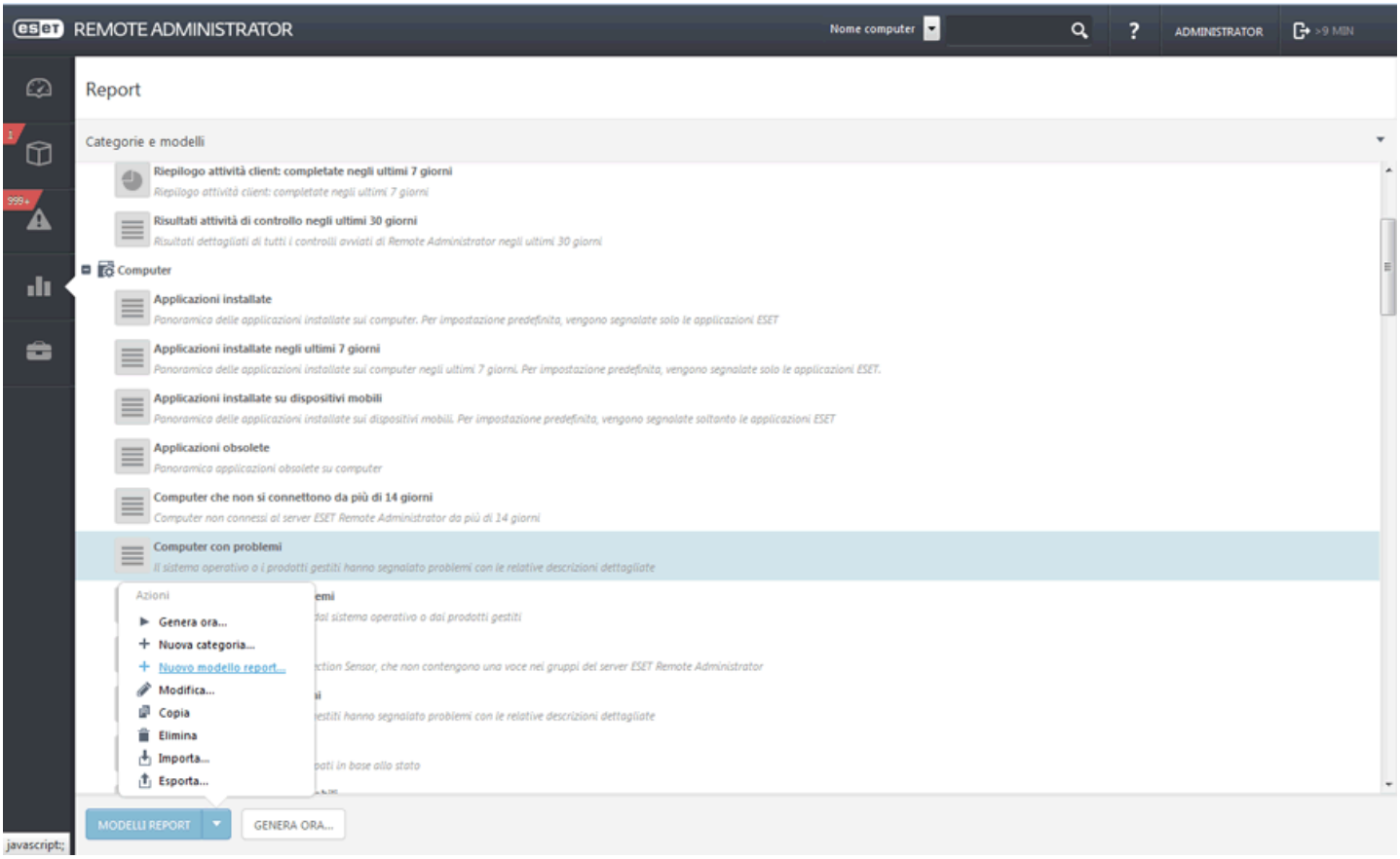
Disattiva

Se si seleziona questa opzione su una minaccia specifica, essa verrà disattivata (il client non verrà disattivato). Il report non verrà più visualizzato come attivo. È anche possibile disattivare il client (seleziona **Disattiva** dal menu contestuale sulla minaccia) che ha segnalato la minaccia.

5.4 Report

I report consentono all'utente di accedere e di filtrare in modo pratico i dati del database. Per garantire un quadro più chiaro, i report vengono suddivisi in categorie contenenti ciascuna una breve descrizione dei report stessi. Fare clic su **Genera ora** nella parte inferiore della pagina per creare e visualizzare un report in base a un modello selezionato.

È possibile utilizzare modelli di report predefiniti dall'elenco di **Categorie e modelli** oppure creare un nuovo modello di report con impostazioni personalizzate. Fare clic su Crea un nuovo modello di report per visualizzare in dettaglio le impostazioni di ciascun report e specificare quelle personalizzate per crearne uno nuovo.



Dopo aver selezionato un report, facendo clic su **Modelli report**, comparirà il menu contestuale **Azioni** nella parte inferiore della pagina. Sono disponibili le seguenti opzioni:

Genera ora... : selezionare un report dall'elenco e accedere a **Modelli report** > **Genera ora...** oppure fare clic semplicemente su **Genera ora...**. Il report verrà generato e sarà possibile rivedere i dati dell'output.

Nuova categoria... : inserire un **Nome** e una **Descrizione** per creare una nuova categoria di modelli di report.

Nuovo modello report...: consente di creare un nuovo modello di report personalizzato.

Modifica...: consente di modificare un modello di report esistente. Le stesse impostazioni e opzioni valgono per la creazione di un nuovo modello di report (vedere il paragrafo precedente).

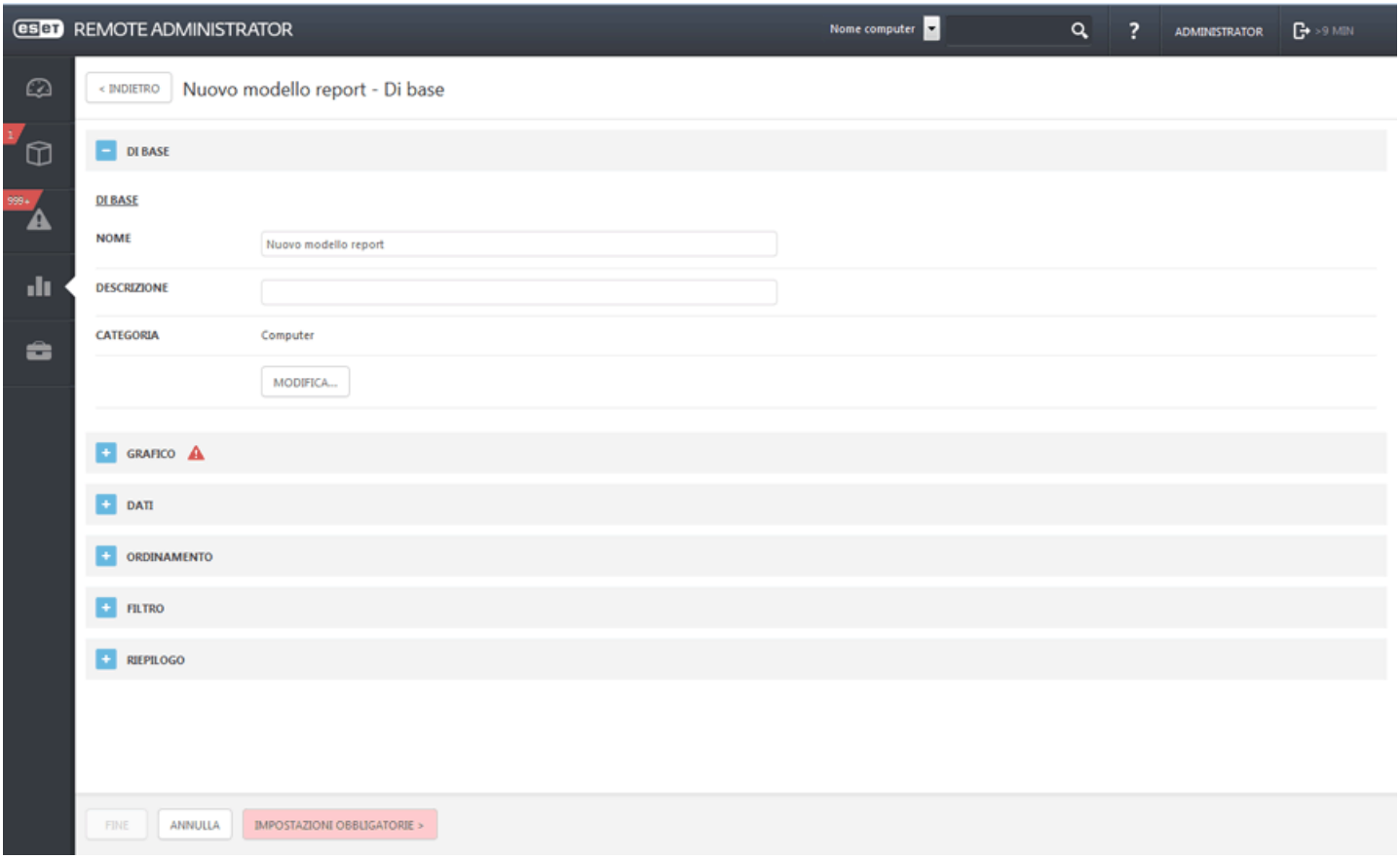
Copia: utilizzare l'opzione Copia solo se si desidera apportare piccole modifiche a un modello di report esistente. **Copiare** un modello di report esistente e **Modificare** le impostazioni per creare un nuovo modello.

Elimina: consente di rimuovere completamente il modello di report selezionato.

Importa/ Esporta: selezionare un report dall'elenco e accedere a **Modelli di report** > **Esporta...**. Il report (contenente i dati definiti) verrà generato e salvato in un file *.txt*.

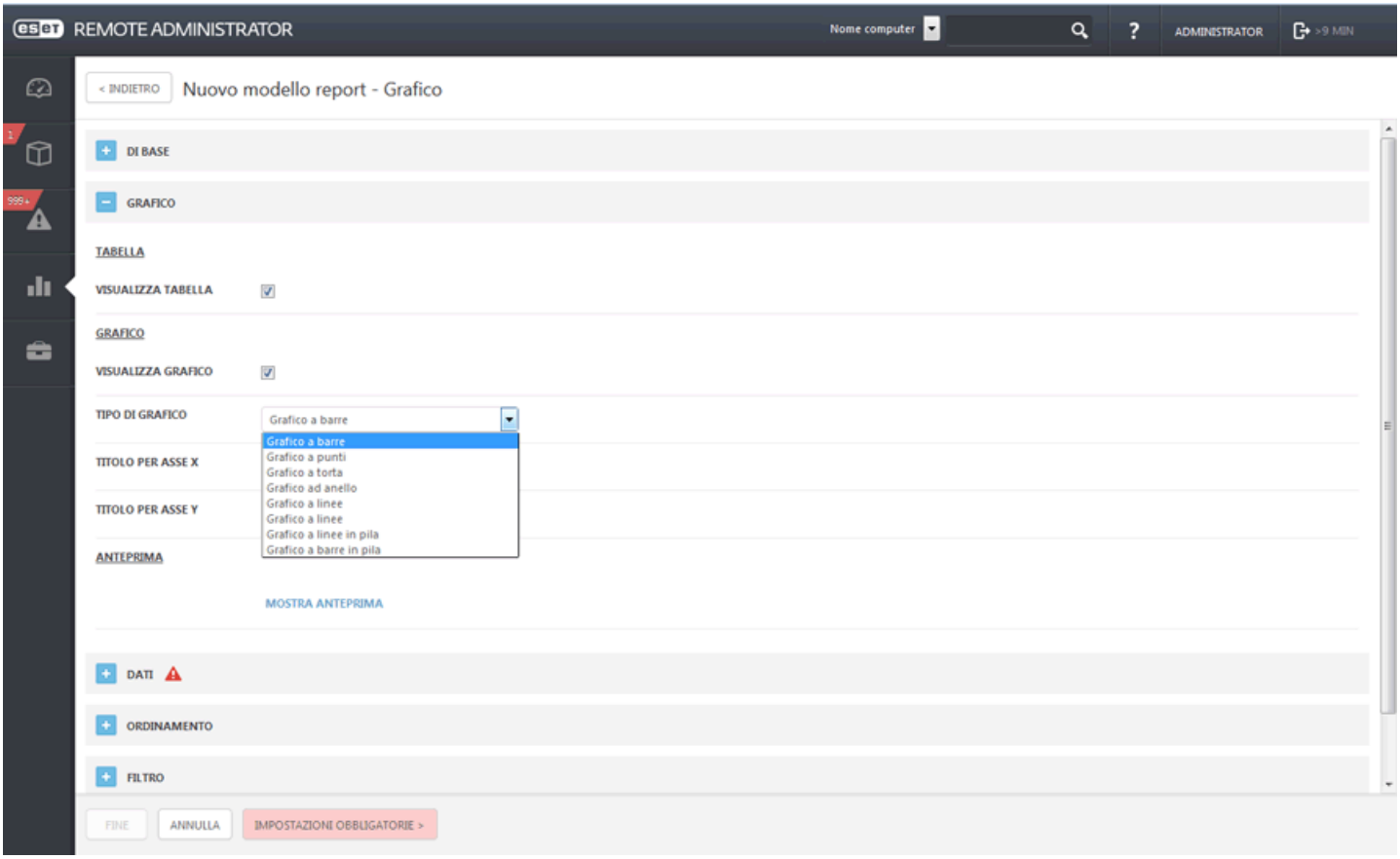
5.4.1 Crea un nuovo modello di report

Accedere a **Report** e fare clic su **Modelli report** sotto a **Categorie e modelli** sulla sinistra. Dalla finestra popup, selezionare **Nuovo modello report...**.



Di base

Modificare le informazioni di base sul modello. Immettere un **Nome**, una **Descrizione** e una **Categoria**. È possibile inserire una categoria predefinita o crearne una nuova (utilizzare l'opzione Nuova categoria descritta nel capitolo precedente).



Grafico

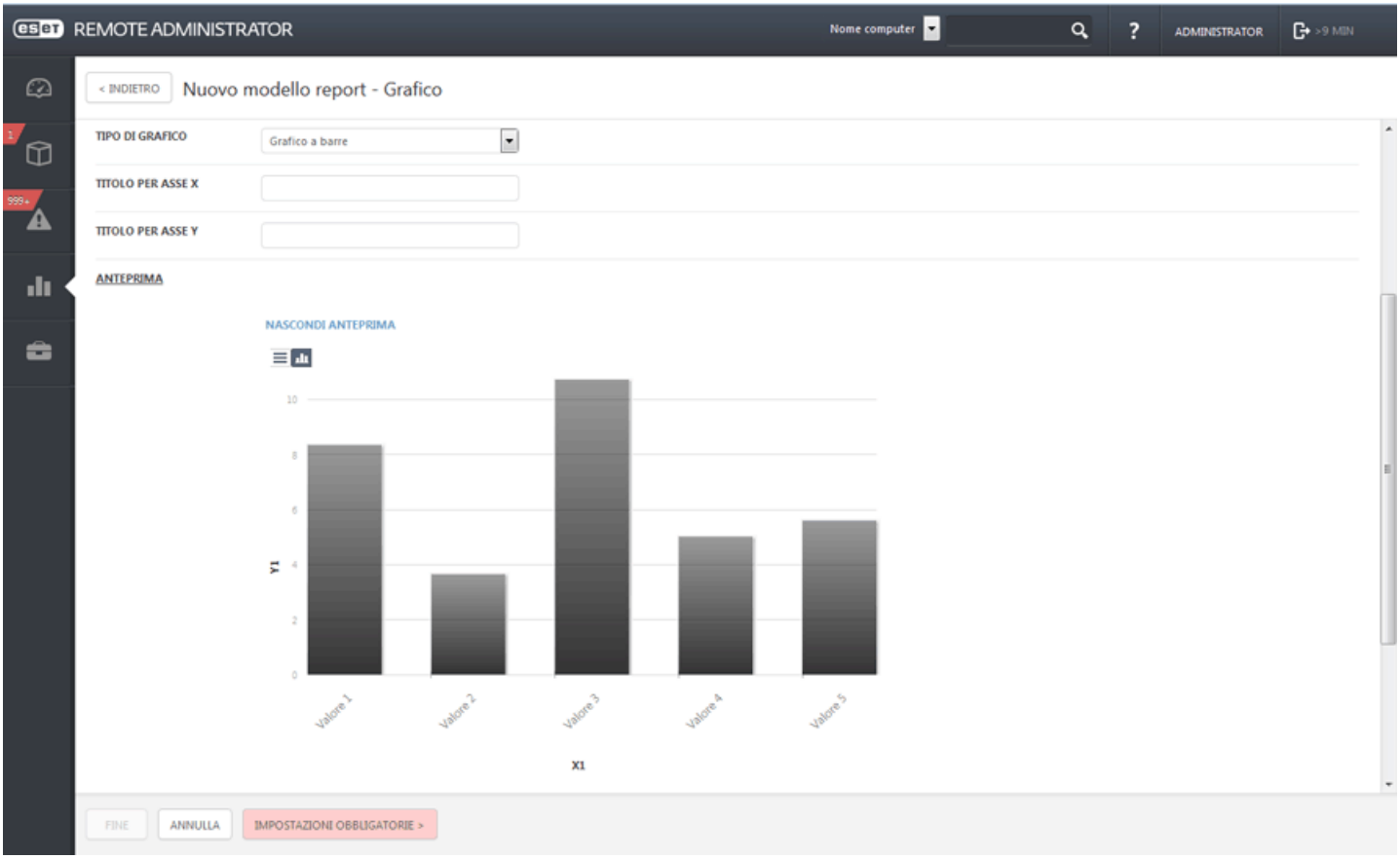
Nella sezione **Grafico**, selezionare il tipo di **Report**. Inserire una **Tabella**, in cui le informazioni sono ordinate in righe e colonne oppure un **Grafico**, in cui i dati sono rappresentati sugli assi X e Y.

NOTA: il tipo di grafico selezionato verrà visualizzato nella sezione **Anteprima**. In tal modo, sarà possibile visualizzare in tempo reale l'aspetto assunto dal report.

Dopo aver selezionato un **Grafico**, è possibile utilizzare varie opzioni:

- **Grafico a barre**: grafico con barre rettangolari la cui lunghezza è proporzionale ai valori rappresentati.
- **Grafico a punti**: in questo grafico, i punti vengono utilizzati per visualizzare i valori quantitativi (il funzionamento è simile a quello del grafico a barre).
- **Grafico a torta**: grafico circolare suddiviso in settori proporzionali, che rappresentano i vari valori.
- **Grafico ad anello**: grafico simile al grafico a torta, da cui si differenzia per il fatto di contenere vari tipi di dati.
- **Grafico a linee**: consente di visualizzare le informazioni come una serie di punti di dati connessi da segmenti di linee rette.
- **Grafico a linee semplici**: consente di visualizzare le informazioni come linee basate su valori senza punti di dati visibili.
- **Grafico a linee in pila**: questo tipo di grafico viene utilizzato se si desidera analizzare i dati con unità di misura diverse.
- **Grafico a barre in pila**: grafico simile a un grafico a barre, dal quale si differenzia per il fatto di contenere vari tipi di dati con diverse unità di misura nelle barre.

Facoltativamente, è possibile inserire un titolo per l'asse **X** e per l'asse **Y** del grafico per renderne più agevoli la lettura e il riconoscimento delle tendenze.



Dati

Nella sezione **Dati**, selezionare le informazioni che si desidera visualizzare:

a. **Colonne tabella**: le informazioni della tabella vengono aggiunte automaticamente in base al tipo di report selezionato. È possibile personalizzare il **Nome**, l'**Etichetta** e il **Formato** (vedere la sezione sottostante).

b. **Assi grafico**: selezionare i dati per l'asse **X** e l'asse **Y**. Facendo clic sui rispettivi simboli, si aprirà una finestra contenente le varie opzioni. Le scelte disponibili per l'asse **Y** dipendono sempre dalle informazioni selezionate per l'asse **X** e viceversa, in quanto sul grafico viene visualizzata la relazione tra questi due elementi. È necessario, inoltre, che i dati siano compatibili. Selezionare le informazioni desiderate, quindi fare clic su **OK**.

È possibile modificare il **Formato** in cui i dati vengono visualizzati in uno qualsiasi dei seguenti:
- **Barra dei dati** (solo per i grafici a barre)/**Valore**/**Colore**/**Icone**

Ordinamento

Aggiungi ordinamento: consente di definire la relazione tra i dati selezionati. Selezionare le informazioni di partenza (valore dell'ordinamento) e il metodo di ordinamento tra **Crescente** e **Decrescente**. Questa operazione definirà il risultato visualizzato nel grafico.

Filtro

Successivamente, definire il metodo di filtraggio. Selezionare il tipo e il valore di filtraggio dall'elenco. Tale operazione definisce le informazioni che verranno visualizzate nel grafico.

Riepilogo

Nel **Riepilogo**, rivedere le opzioni e le informazioni selezionate. Se le informazioni sono corrette, fare clic su **Fine** per creare un Modello di report.

Ogni report presente nel dashboard contiene le proprie opzioni di personalizzazione: fare clic sul simbolo a forma di rotella nell'angolo in alto a destra per visualizzarle. Da qui, è possibile **Aggiornare** le informazioni visualizzate, **Passare** a un altro report, **Modificare** il modello del report (vedere le opzioni precedenti), impostare un nuovo intervallo di **Aggiornamento** che definisce la frequenza di aggiornamento dei dati contenuti nel report o **Rinominare**/**Rimuovere** il report. Utilizzando le frecce nel simbolo sottostante, è possibile personalizzare le dimensioni del report. È possibile ingrandire i report più rilevanti, rimpicciolire quelli meno rilevanti e così via. Fare clic su **Passa a schermo interno** per visualizzare un report in modalità schermo intero.

5.4.2 Genera report

Un modello può essere creato o modificato in due modi:

1. Accedere ad **Amministrazione** > **Attività** > **Attività server**. Selezionare **Nuova...** per creare una nuova attività Genera report.
2. Selezionare un modello a partire dal quale si desidera generare un report. È possibile utilizzare e modificare un modello di report predefinito o creare un nuovo modello di report.

- È possibile inviare il report tramite e-mail (in un formato di file definito qui) o salvarlo direttamente su un file. Facendo clic su una delle opzioni sarà possibile visualizzare le impostazioni corrispondenti indicate di seguito.
- Configurare le impostazioni (in base a quanto descritto nell'attività Genera report) e fare clic su **Fine**.
- L'attività è stata creata e verrà visualizzata nell'elenco **Tipi di attività**. Selezionare l'attività e fare clic su **Esegui ora** nella parte inferiore della pagina. L'attività verrà eseguita immediatamente.

5.4.3 Pianifica un report

1. Accedere a **Amministrazione** > **Attività** > **Attività server**. Selezionare **Nuova** per creare una nuova attività **Genera report**.
2. Selezionare un modello a partire dal quale si desidera generare un report. È possibile utilizzare e modificare un modello di report predefinito o creare un nuovo modello di report.

- È possibile inviare il report tramite e-mail (in un formato di file definito qui) o salvarlo su un file. Facendo clic su una delle opzioni sarà possibile visualizzare le impostazioni corrispondenti indicate di seguito.
- Configurare le impostazioni (in base a quanto descritto nell'attività Genera report). A questo punto, verrà creata un'**Attivazione server** per l'attività specifica.
- Nella sezione **Attivazione**, accedere a **Impostazioni**. Selezionare **Attivazione pianificata** e il momento in cui si desidera eseguire l'attività.
- Fare clic su **Fine**. L'attività verrà creata ed eseguita nel periodo definito qui (una volta o ripetutamente).

5.4.4 Applicazioni obsolete

Per visualizzare i componenti ERA obsoleti, utilizzare il report chiamato **Applicazioni obsolete**.

È possibile eseguire l'operazione in due modi:

1. Aggiungendo un nuovo dashboard e facendo clic su uno dei riquadri, che consentirà di visualizzare una schermata popup in cui sono elencati i **Modelli di report**. Selezionando un report **Applicazioni obsolete** dall'elenco e facendo clic su **Aggiungi**.
2. Accedere a **Report**, quindi alla categoria **Computer**, selezionare il modello **Applicazioni obsolete** dall'elenco e fare clic sul pulsante **Genera ora...** in fondo. Il report verrà generato e sarà possibile rivedere i dati dell'output.

Per effettuare l'aggiornamento dei componenti, utilizzare l'attività client Aggiornamento componenti amministratore.

6. Amministrazione di ESET Remote Administrator

La sezione Amministrazione di ESET Remote Administrator illustra le modalità di gestione e di configurazione di ESET Remote Administrator. Per ulteriori informazioni, consultare il capitolo Amministrazione.

6.1 Amministrazione

La sezione **Amministrazione** rappresenta il principale componente di configurazione di ESET Remote Administrator. Questa sezione contiene tutti gli strumenti utili all'amministratore per la gestione delle soluzioni di protezione client, nonché delle impostazioni del server ERA. È possibile utilizzare gli strumenti Amministrazione per configurare l'ambiente di rete in modo da ridurre il numero di interventi di manutenzione. È inoltre possibile configurare le notifiche e i dashboard che consentono di aggiornare l'utente sullo stato della rete.

In questa sezione

- Modelli gruppi dinamici
- Gruppi
- Criteri
- Attività client
- Attività server
- Attivazioni
- Notifiche
- Certificati del peer
- Diritti di accesso
- Impostazioni server
- Gestione licenza

6.1.1 Gruppi

I gruppi consentono di gestire e classificare i computer. È quindi possibile applicare facilmente varie impostazioni, attività o restrizioni ai computer client, in base alla relativa presenza all'interno di uno specifico gruppo. L'utente può utilizzare gruppi e modelli di gruppi predefiniti oppure crearne di nuovi.

Sono disponibili due tipi di gruppi client:

Gruppi statici

I Gruppi statici sono gruppi di computer client selezionati (membri), i cui membri sono statici, possono essere solo aggiunti/rimossi manualmente e non sono basati su criteri dinamici. Un computer può appartenere a un solo Gruppo statico.

Gruppi dinamici

I Gruppi dinamici sono gruppi di client la cui appartenenza al gruppo è determinata da criteri specifici. Se un client non soddisfa tali criteri, verrà rimosso dal gruppo. I computer che soddisfano i criteri verranno aggiunti manualmente al gruppo.

La finestra **Gruppi** è suddivisa in tre sezioni:

1. Un elenco di tutti i gruppi e dei relativi sottogruppi viene visualizzato sulla sinistra. È possibile selezionare un gruppo e un'azione a esso relativa dal menu contestuale (rotella accanto al nome del gruppo). Le opzioni sono identiche a quelle descritte di seguito (pulsante Azioni gruppo).

2. I dettagli relativi al gruppo selezionato sono visualizzati nel riquadro sulla destra (è possibile passare da una scheda all'altra):

- **Computer** appartenenti al gruppo.
- **Criteri** assegnati al gruppo.
- **Attività** assegnate al gruppo.
- **Riepilogo**: descrizione di base del gruppo.

3. I pulsanti del menu popup **Gruppi** e **Computer** consentono di eseguire tutte le seguenti azioni:

Pulsante azioni gruppi

+ Nuovo gruppo statico...
Questa opzione diventa disponibile facendo clic su un **Gruppo** nell'elenco sulla sinistra. Questo gruppo sarà il gruppo padre predefinito. Tuttavia, è possibile modificarlo in un momento successivo durante la creazione di un nuovo gruppo statico.

+ Nuovo gruppo dinamico...
Questa opzione diventa disponibile facendo clic su un **Gruppo** nell'elenco sulla sinistra. Questo gruppo sarà il gruppo padre predefinito. Tuttavia, è possibile modificarlo in un momento successivo in seguito alla creazione di un nuovo gruppo dinamico.

Modifica...
Consente all'utente di modificare il gruppo selezionato. Le stesse impostazioni valgono per la creazione di un nuovo gruppo (statico o dinamico).

Sposta...
È possibile selezionare un gruppo e spostarlo come sottogruppo di un altro gruppo.

Elimina
Rimuove completamente il gruppo selezionato.

Importa...
È possibile importare un elenco (solitamente un file di testo) di computer come membri del gruppo selezionato. Se i computer sono già esistenti come membri del gruppo, il conflitto verrà risolto in base all'azione selezionata:

- **Ignora computer in conflitto** (i computer in conflitto non verranno aggiunti)
- **Sposta i computer in conflitto da altri gruppi** (i computer in conflitto provenienti da altri gruppi verranno spostati qui)
- **Duplica computer in conflitto** (i computer in conflitto verranno aggiunti, ma con nomi diversi).

Esporta...
Esporta i membri del gruppo (e dei sottogruppi, se selezionati) in un elenco (file *.txt*). Questo elenco può essere utilizzato per scopi di revisione oppure importato in un momento successivo.

+ Aggiungi nuovo...
Questa opzione consente all'utente di aggiungere un nuovo dispositivo.

Controlla
L'utilizzo di questa opzione consentirà di eseguire l'attività Controllo su richiesta sul client che ha segnalato la minaccia.

Aggiorna DB firme antivirali
L'utilizzo di questa opzione consentirà di eseguire l'attività Aggiornamento del database delle firme antivirali (attiva manualmente un aggiornamento).

Mobile

- **Registra...** : questa opzione consente all'utente di creare una nuova attività client.
- **Trova** : opzione che consente di richiedere le coordinate GPS del dispositivo mobile.
- **Blocca**: il dispositivo verrà bloccato in caso di rilevamento di un'attività sospetta oppure nel caso in cui sia contrassegnato come mancante.
- **Sblocca** : il dispositivo verrà sbloccato.
- **Sirena** : attiva da remoto una sirena ad alto volume, anche se il dispositivo è in modalità silenziosa.
- **Cancella**: verranno cancellati definitivamente tutti i dati memorizzati sul dispositivo.

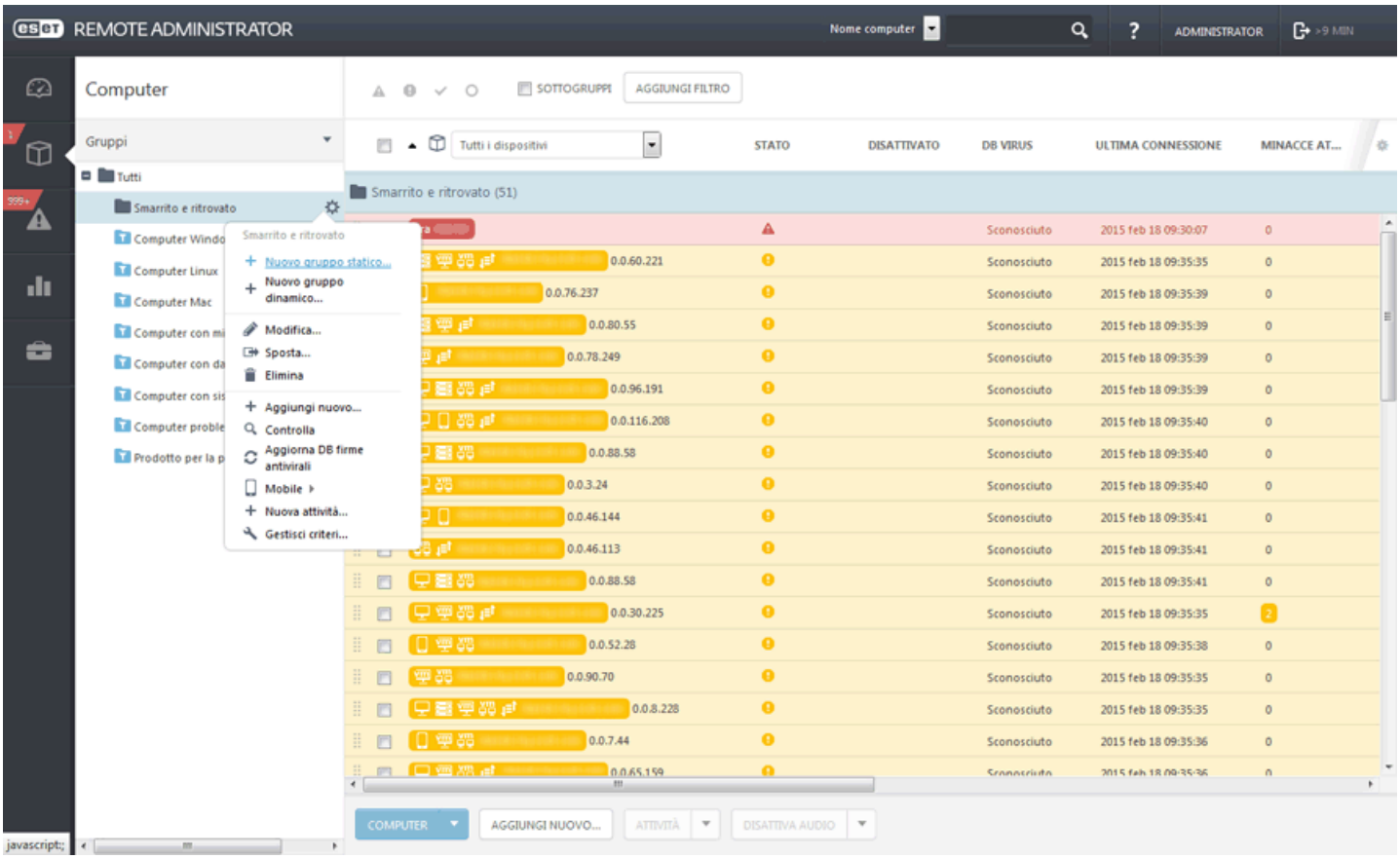
+ Nuova attività...
È possibile creare una nuova Attività client. Selezionare un'attività e configurare la limitazione delle richieste (facoltativo). L'attività verrà accodata in base alle relative impostazioni.
Questa opzione attiva immediatamente un'attività esistente che l'utente seleziona da un elenco di attività disponibili. L'attivazione non è disponibile per questa attività, in quanto verrà eseguita immediatamente.

Gestisci criteri...
Assegnare un Criterio al gruppo selezionato.

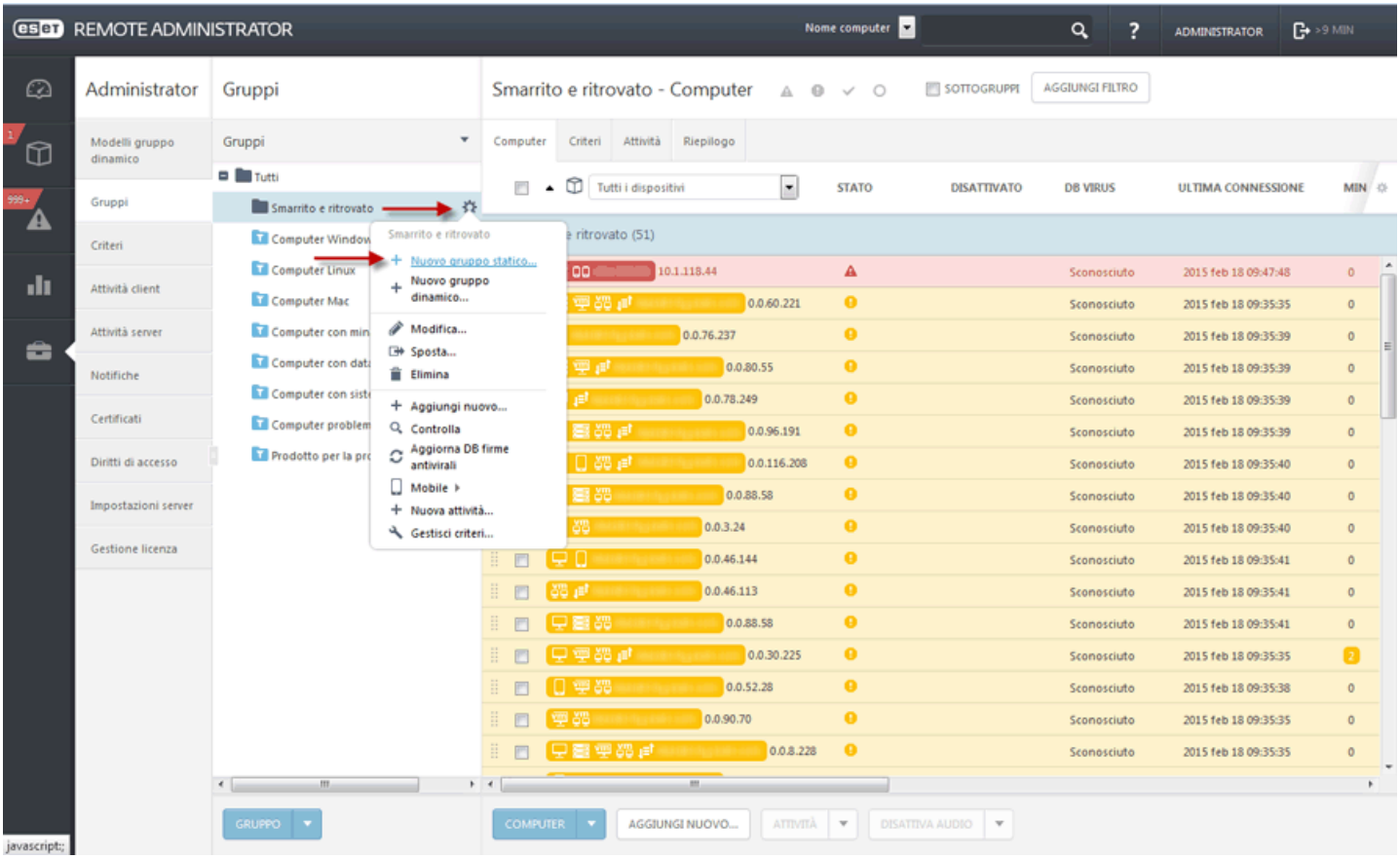
6.1.1.1 Crea nuovo gruppo statico

Per creare un nuovo gruppo statico, è possibile utilizzare una delle tre seguenti modalità:

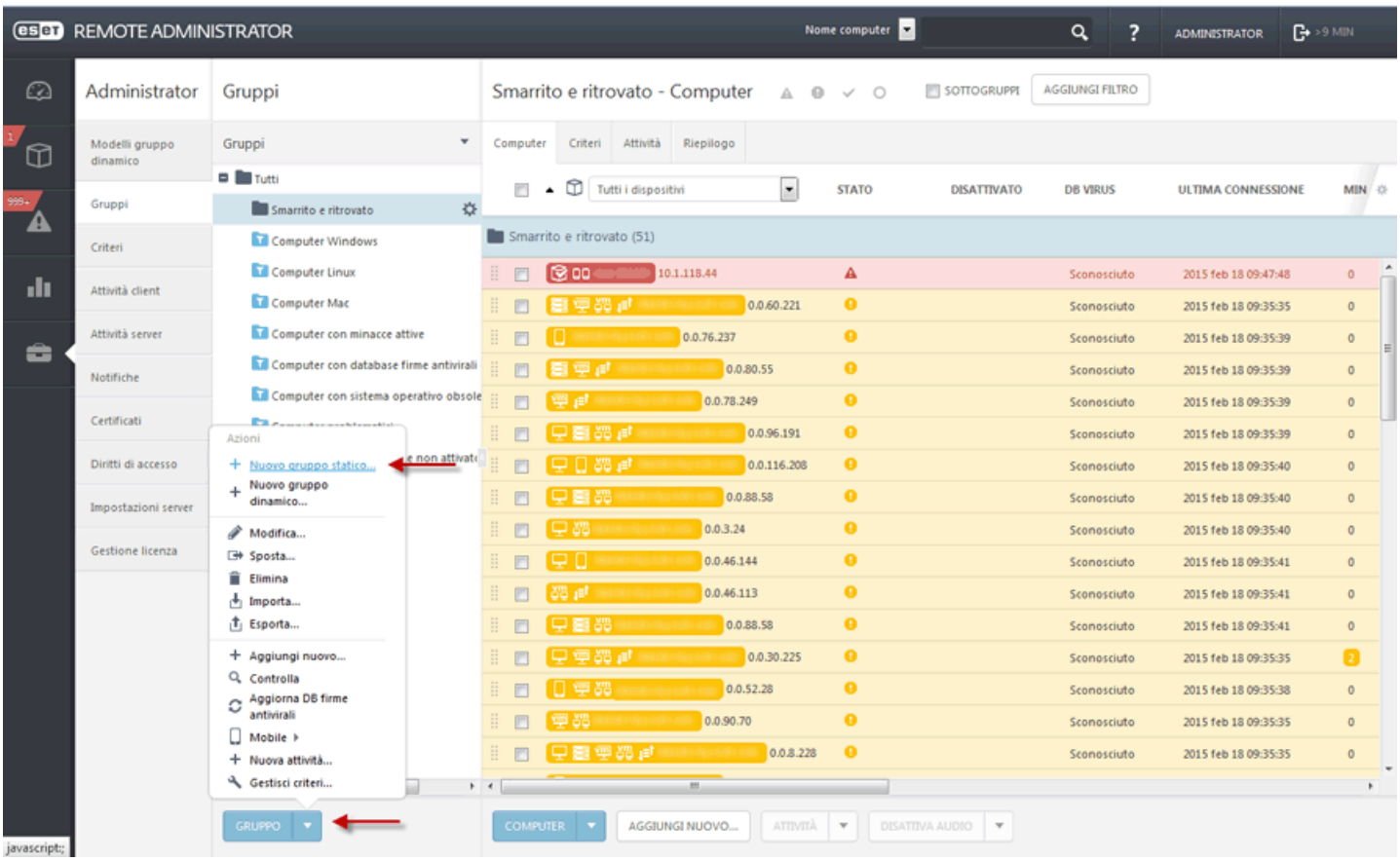
1. Fare clic su **Computer** > **Gruppi** > ⚙ e selezionare **Nuovo gruppo statico...**



2. Fare clic su **Amministrazione** > **Gruppi** > ⚙ > **Nuovo gruppo statico...**

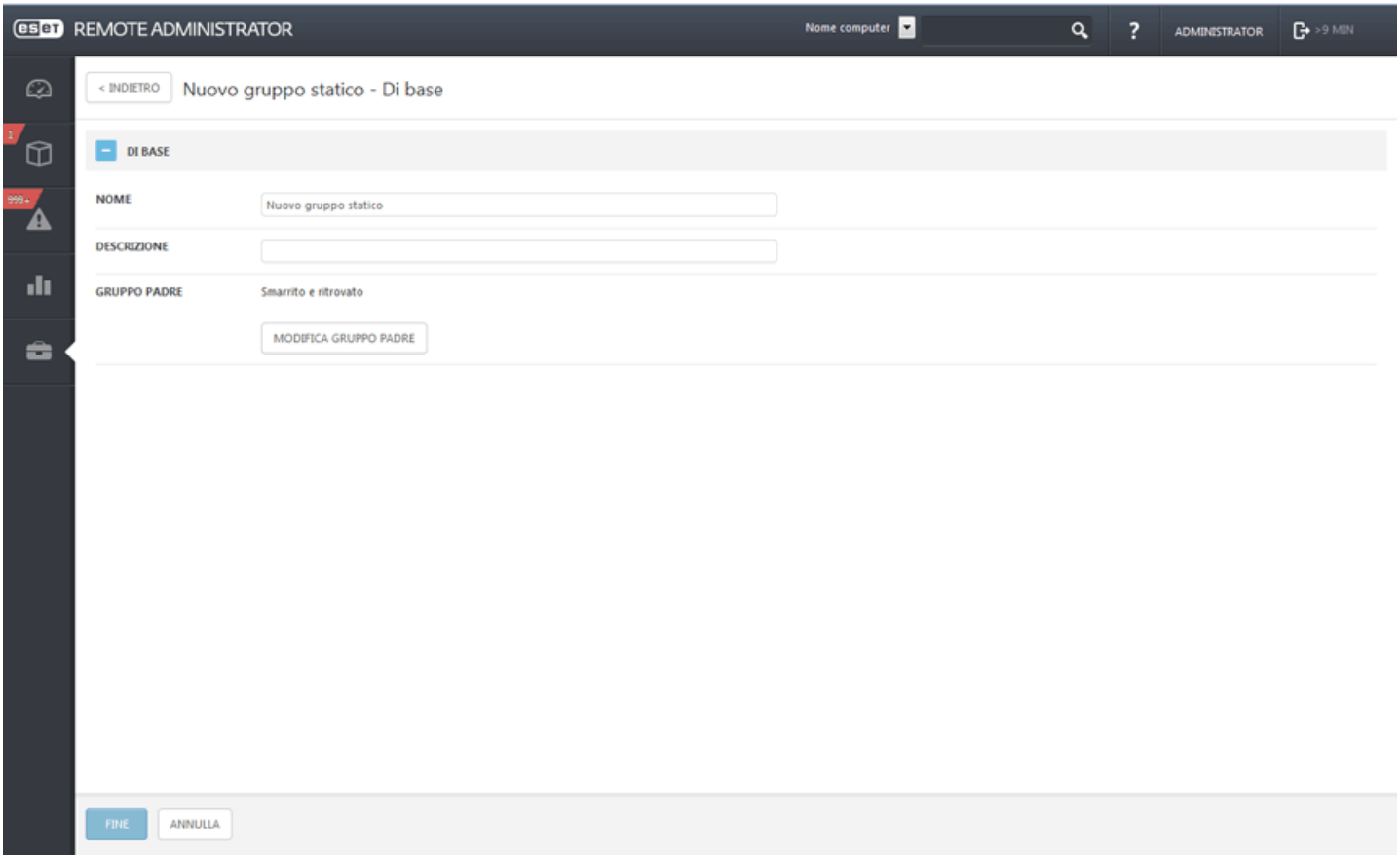


3. Fare clic su **Amministrazione** > **Gruppi** >, selezionare un Gruppo statico e fare clic su **Gruppo**..



Di base

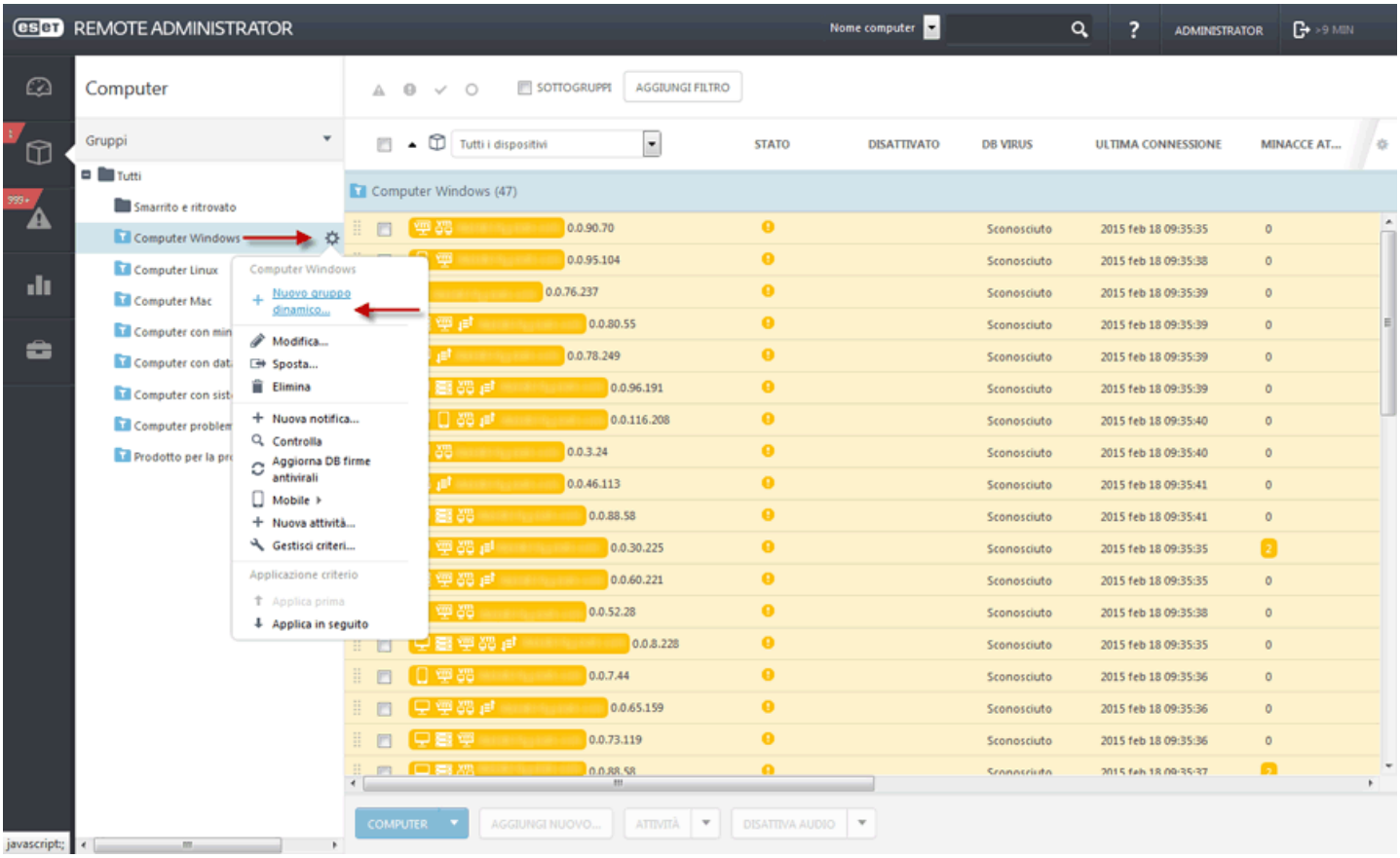
Immettere un **Nome** e una **Descrizione** (facoltativa) per il nuovo Gruppo statico. Per impostazione predefinita, il gruppo padre è il gruppo selezionato dall'utente nella fase iniziale della creazione del nuovo gruppo statico. Per modificare il gruppo padre, fare clic su **Modifica gruppo padre** e selezionare un gruppo padre nella struttura. Il padre del nuovo gruppo statico deve essere un gruppo statico, poiché non è possibile che un gruppo dinamico abbia gruppi statici. Fare clic su **Fine** per creare il nuovo gruppo statico.



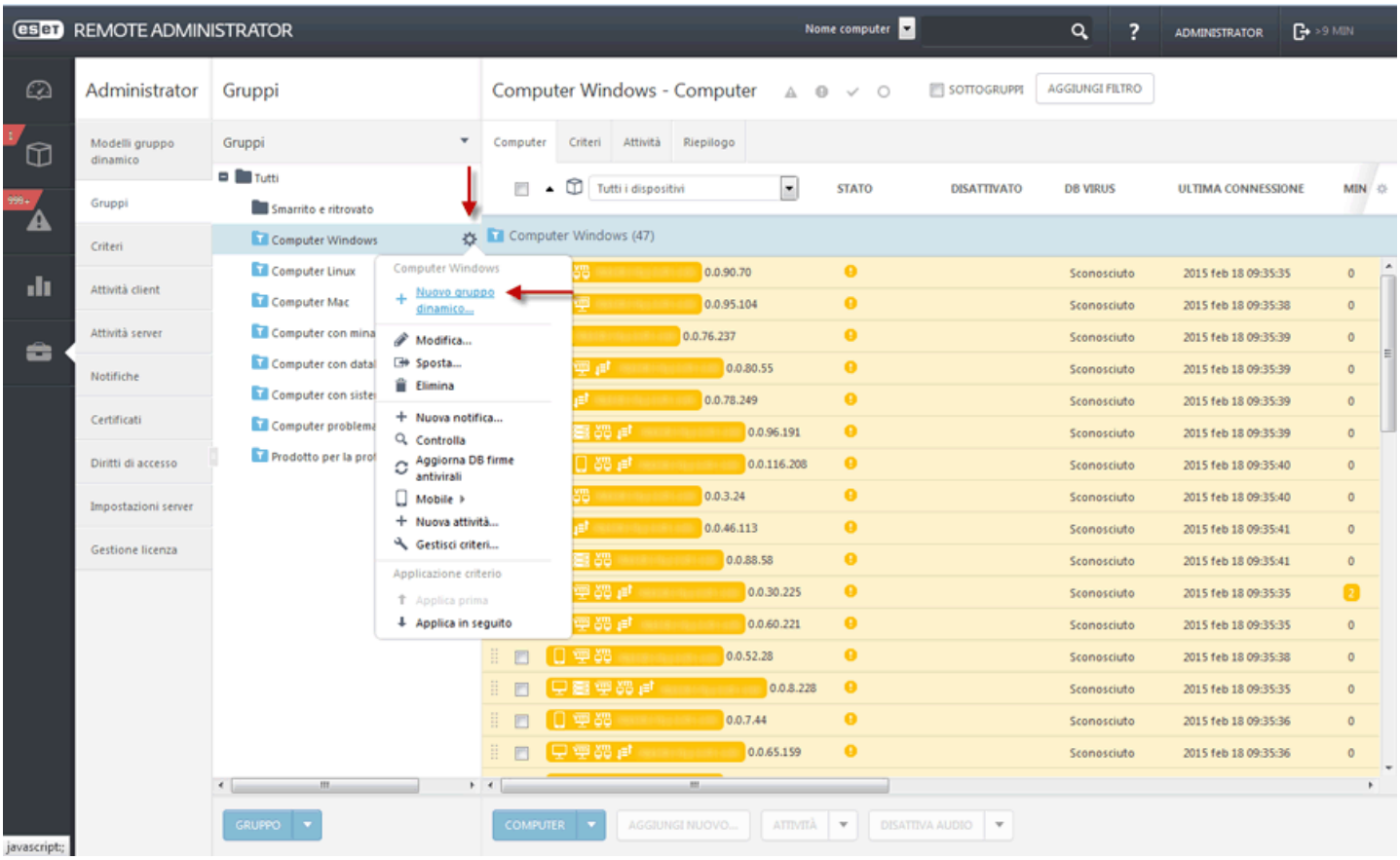
6.1.1.2 Crea nuovo gruppo dinamico

Per creare un nuovo gruppo dinamico, è possibile utilizzare una delle tre seguenti modalità:

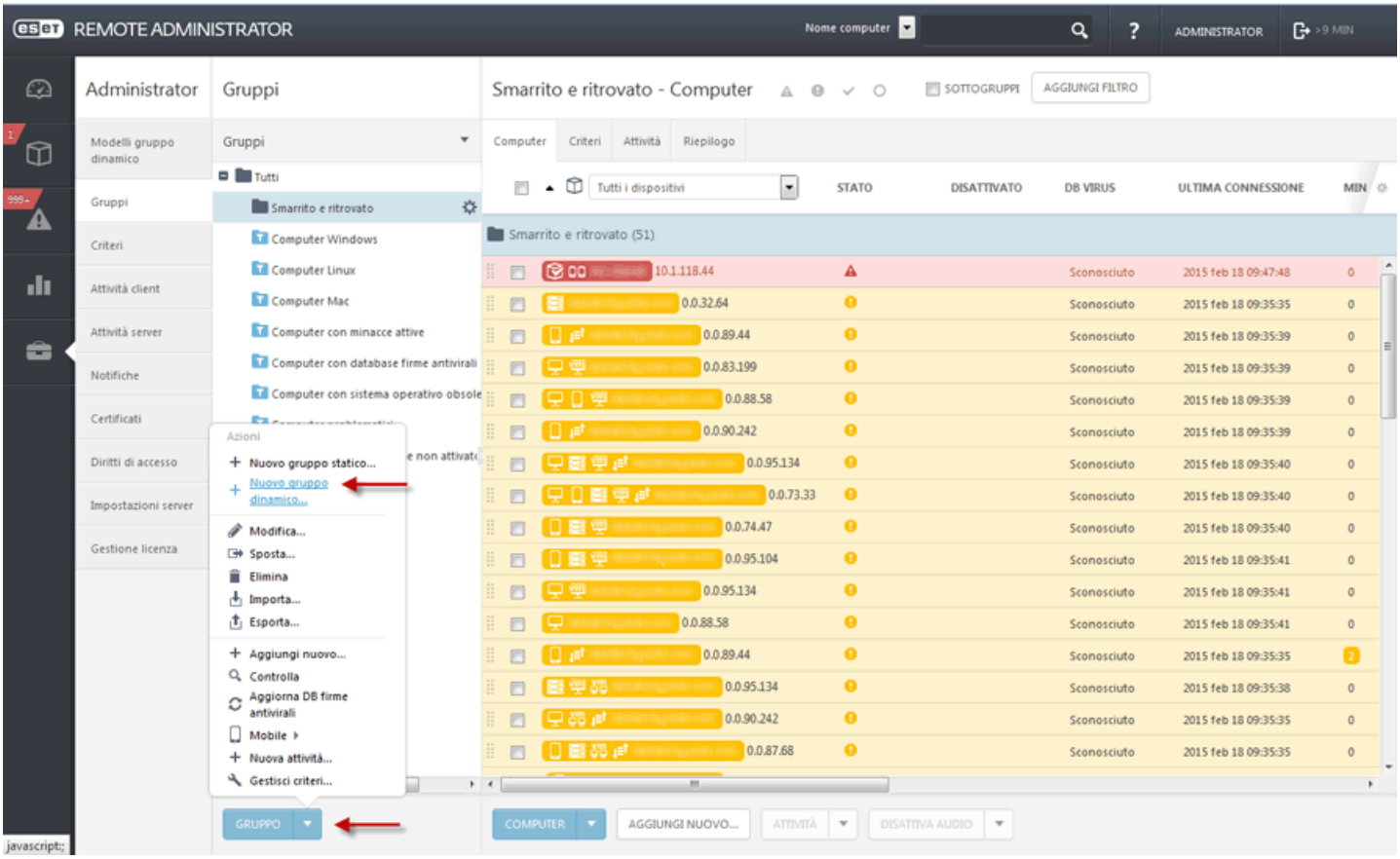
1. Fare clic su **Computer** > **Gruppi** > ⚙ e selezionare **Nuovo gruppo dinamico...**



2. Fare clic su **Amministrazione** > **Gruppi** > ⚙ > **Nuovo sottogruppo dinamico...**



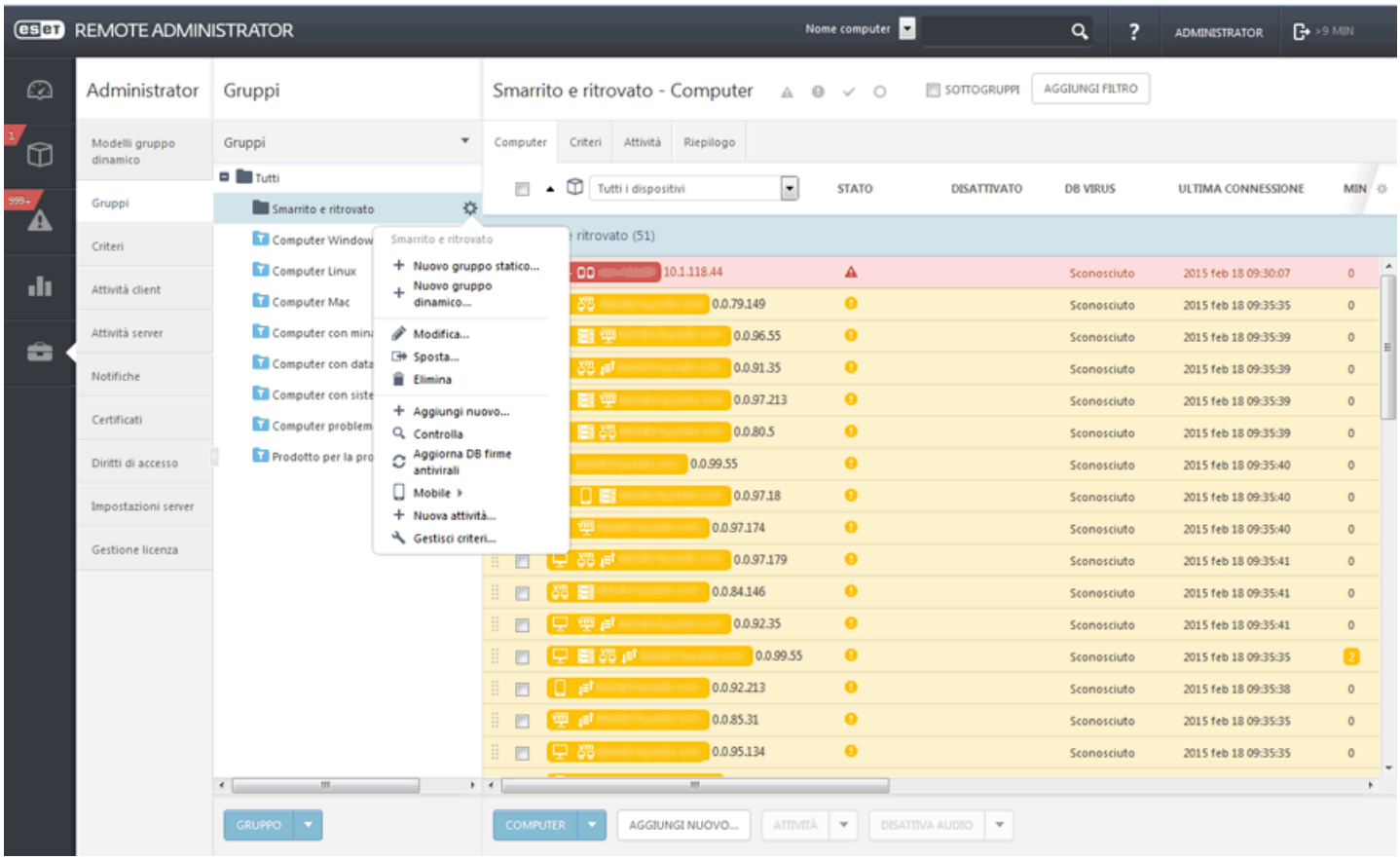
3. Fare clic su **Amministrazione** > **Gruppi** > Fare clic sul pulsante **Gruppo**, quindi su **Nuovo gruppo dinamico...**



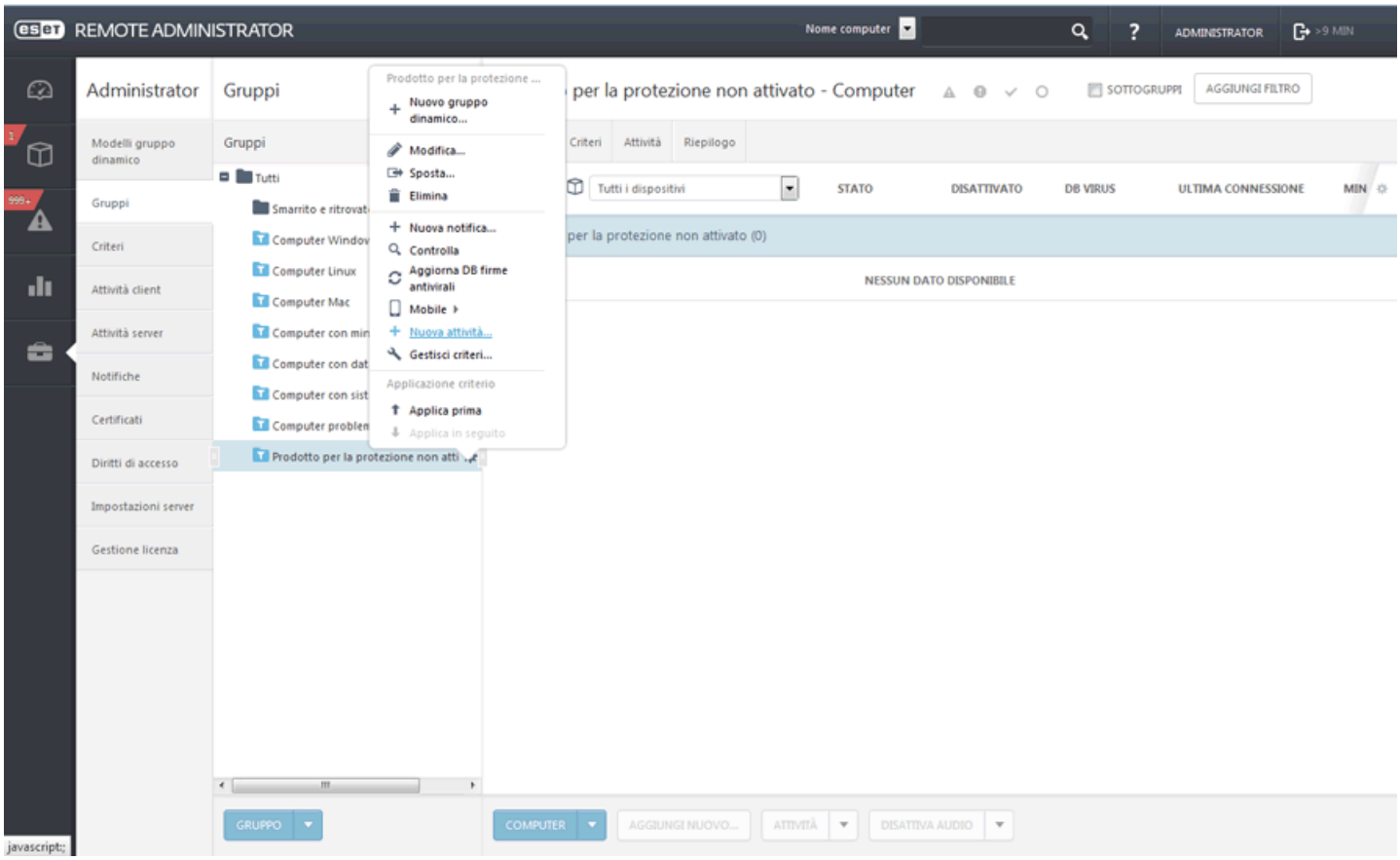
Verrà visualizzata una Procedura guidata nuovo gruppo dinamico.

6.1.1.3 Assegna attività a un gruppo

Fare clic su **Amministrazione** > **Gruppi** > selezionare gruppo **Statico** o **Dinamico** > ⚙ accanto al gruppo selezionato, oppure fare clic su **Gruppo** > **+ Nuova attività**



La stessa procedura può essere eseguita da **Computer**, selezionare **Statico** o **Dinamico** e fare clic su ⚙ > **+ Nuova attività**

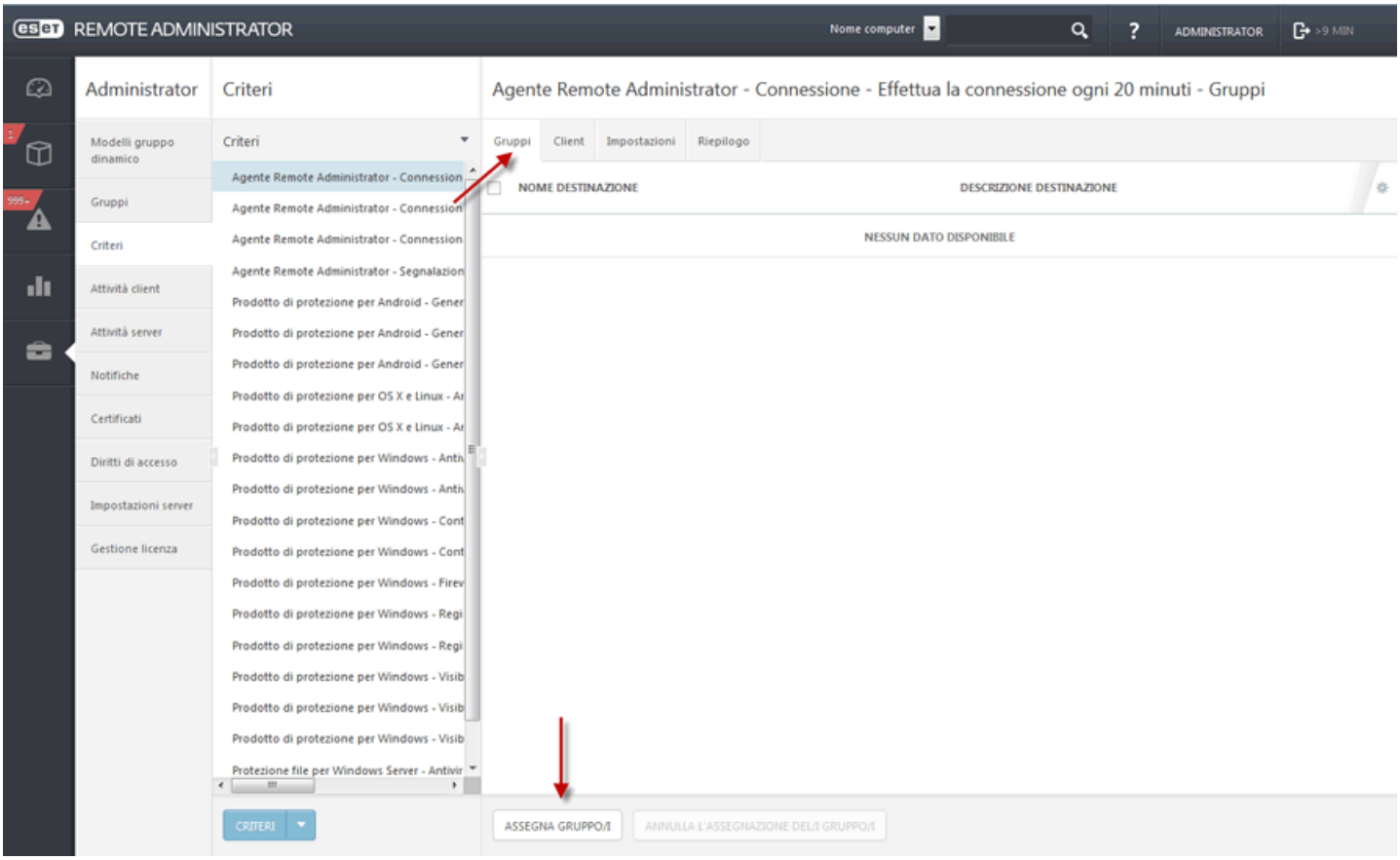


Verrà visualizzata una finestra della Procedura guidata nuova attività client.

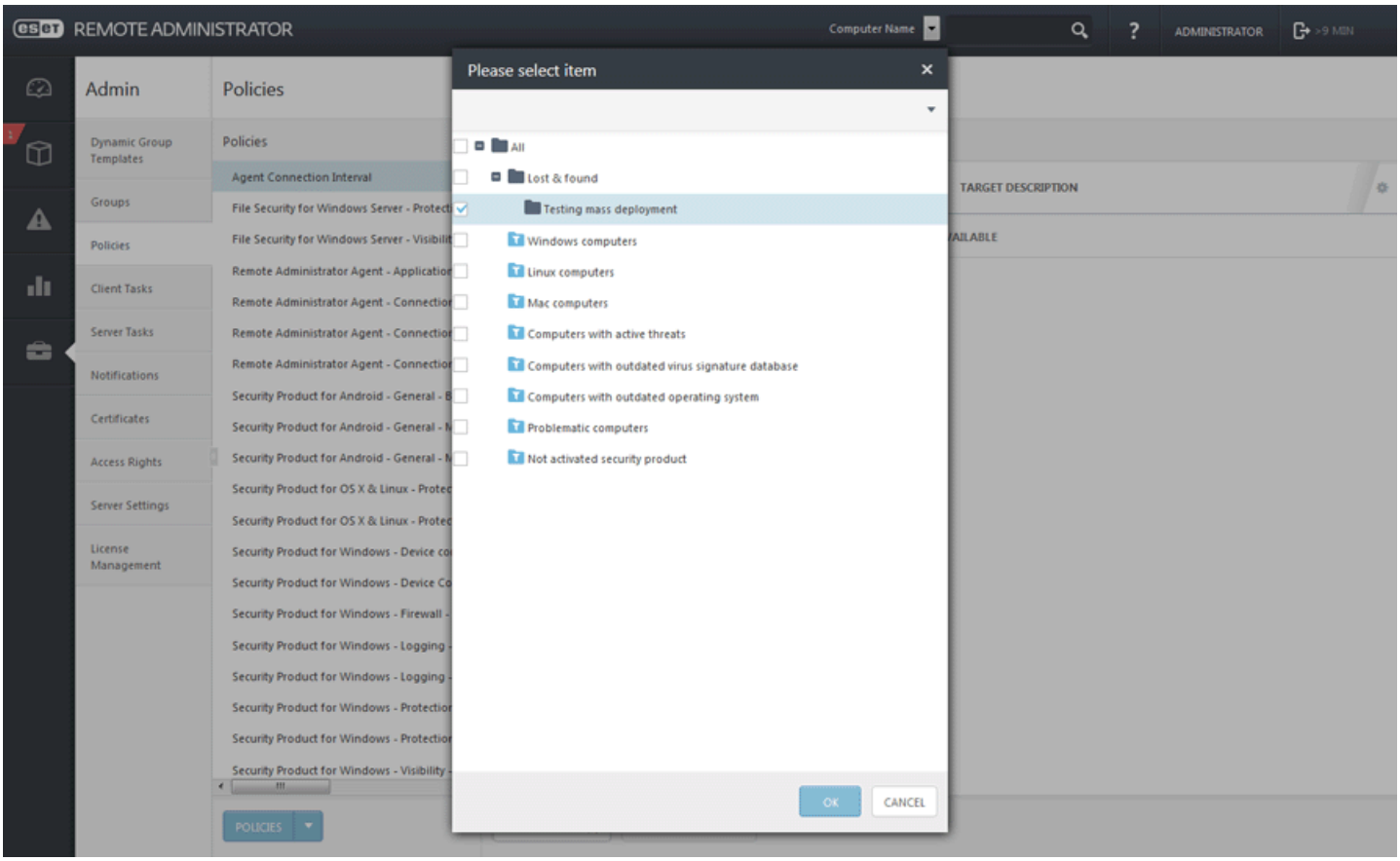
6.1.1.4 Assegna un criterio a un gruppo

Dopo aver creato un criterio, l'utente può assegnarlo a un **Gruppo statico** o **dinamico**. Un criterio può essere assegnato in due modi:

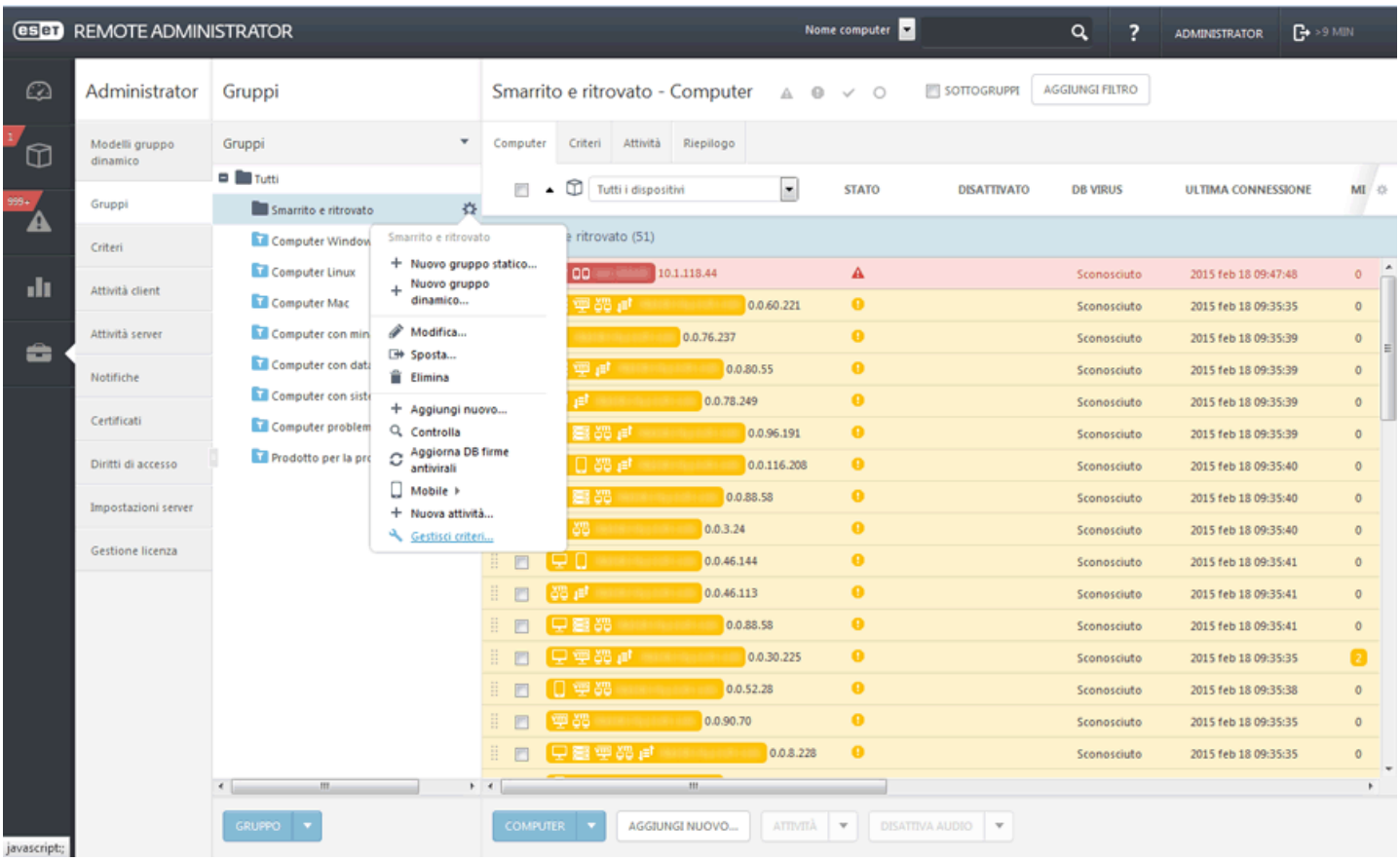
1. In **Amministrazione** > **Criteri** > selezionare un criterio e fare clic su **Assegna gruppo/i**. Selezionare un gruppo statico o dinamico e fare clic su **OK**.



Selezionare un **Gruppo** dall'elenco.



2. Fare clic su **Amministrazione** > **Gruppi** > **Gruppo** oppure sull'icona a forma di rotella accanto al nome del gruppo e selezionare **Gestisci criteri**.



Nella finestra **Ordine applicazione criterio** fare clic su **Aggiungi criterio**. Selezionare la casella di controllo accanto al criterio che si desidera assegnare al gruppo e fare clic su **OK**.
Fare clic su **Salva**. Per visualizzare i criteri assegnati a un gruppo specifico, selezionarlo e fare clic sulla scheda **Criteri** per aprire un elenco di criteri assegnati al gruppo.

NOTA: per ulteriori informazioni sui criteri, consultare il capitolo Criteri.

6.1.1.5 Criteri e gruppi

L'appartenenza di un computer nel Gruppo dinamico è determinata da criteri assegnati a tale computer. È inoltre determinata dal modello sul quale si basa il gruppo dinamico.

6.1.1.6 Gruppi statici

- I gruppi statici vengono utilizzati per ordinare manualmente i computer client in **gruppi** e **sottogruppi**. L'utente può creare Gruppi statici personalizzati e spostarvi i computer desiderati.
- I gruppi statici possono essere creati solo manualmente. È quindi possibile spostare manualmente i computer client in tali gruppi. Ciascun computer può appartenere solo a un gruppo statico.

Sono presenti due Gruppi statici predefiniti:

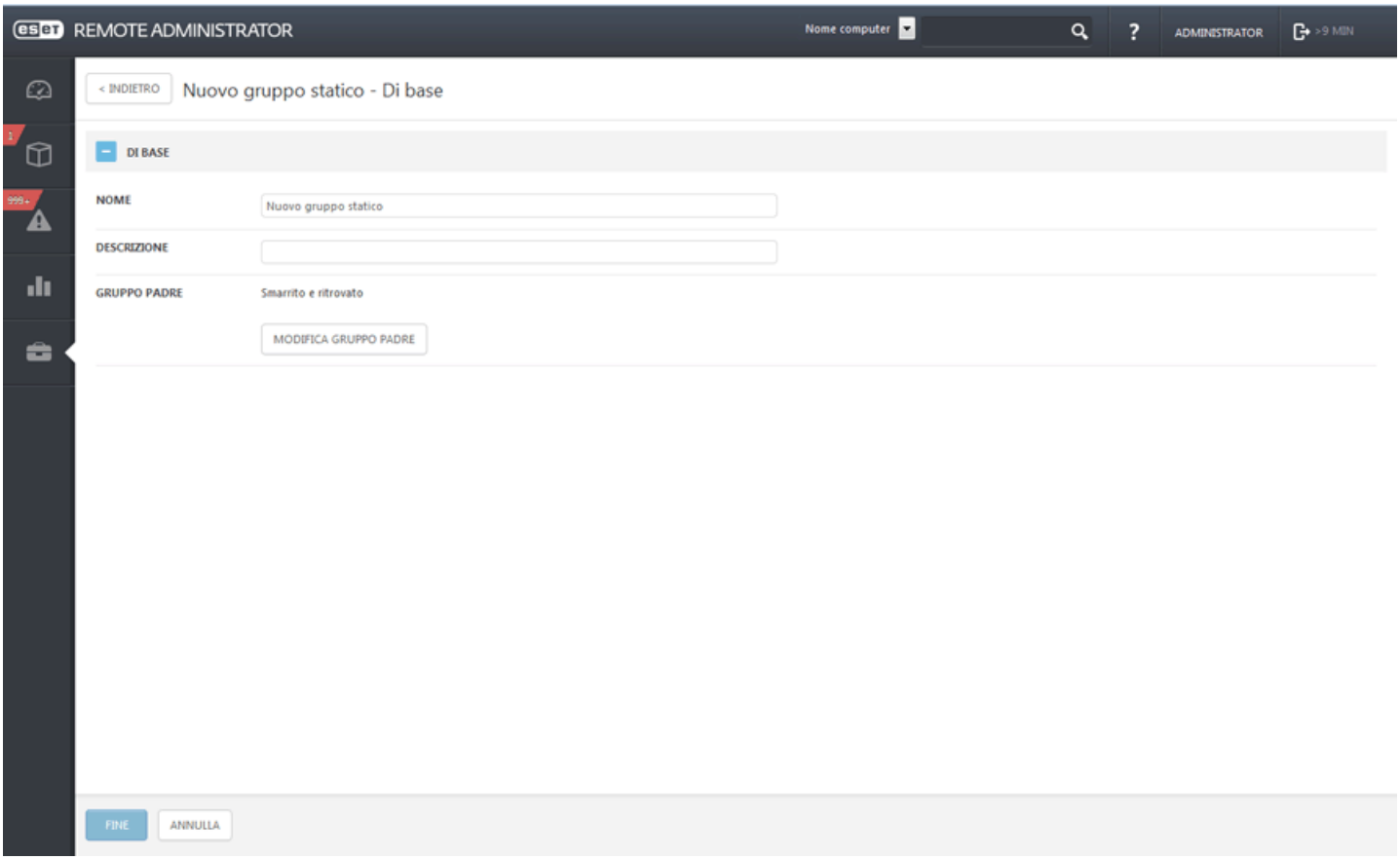
- **Tutti:** gruppo principale per tutti i computer nella rete dei server ERA. che viene utilizzato per applicare i criteri di ciascun computer come criteri predefiniti. Il gruppo viene visualizzato sempre e all'utente non è consentito modificarne il nome attraverso la modifica del gruppo stesso.
- **Smarrito e ritrovato** come gruppo figlio del gruppo **Tutti**: ciascun nuovo computer che connette per la prima volta l'agente al server viene visualizzato automaticamente in questo gruppo. Il gruppo può essere rinominato e copiato ma non eliminato o spostato.

6.1.1.6.1 Procedura guidata gruppo statico

In **Computer** > **Gruppi**, selezionare uno dei Gruppi statici, fare clic sulla rotella⚙, quindi selezionare **Nuovo gruppo statico.**

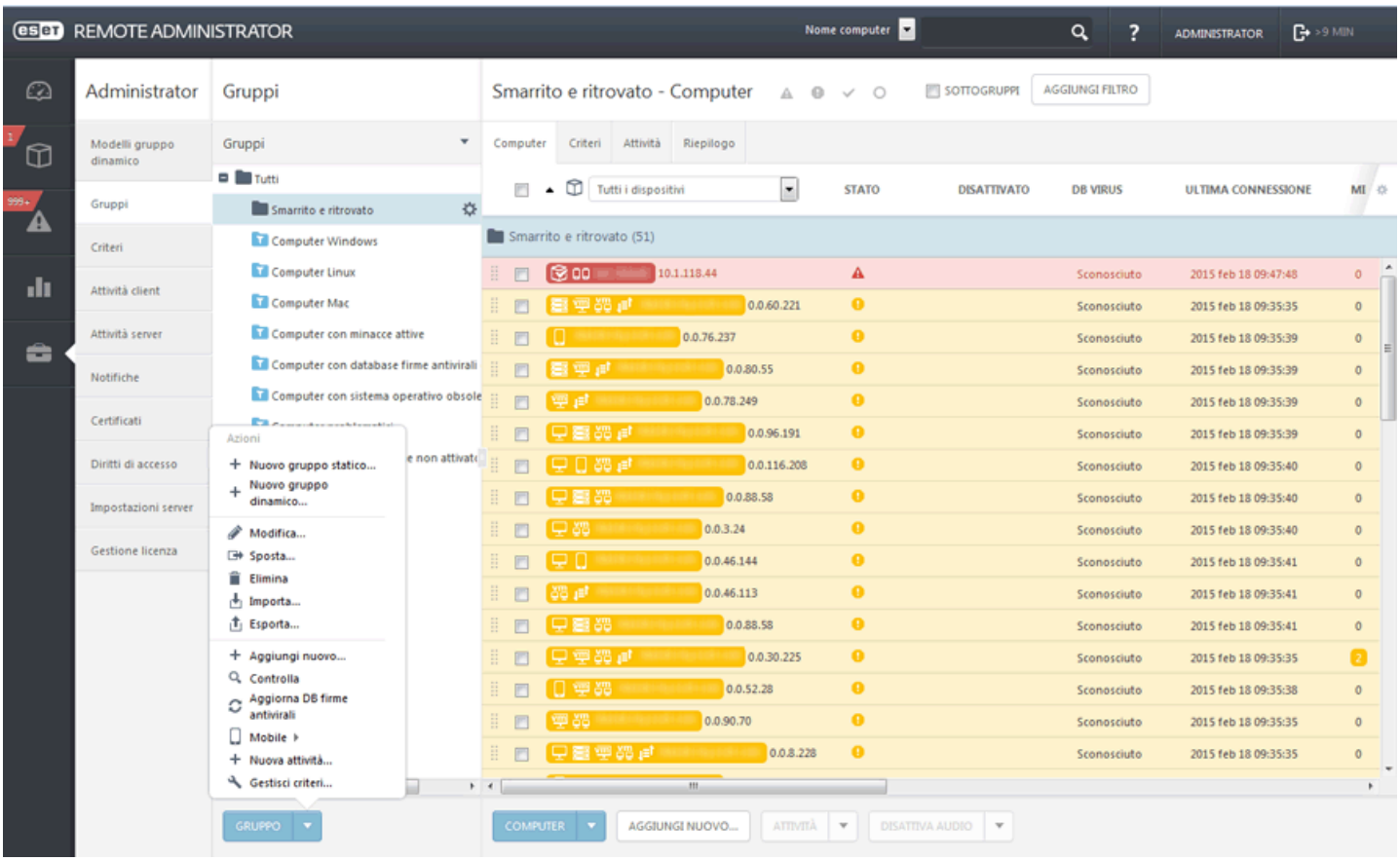
Di base

Immettere un **Nome** e una **Descrizione** per il nuovo gruppo. Facoltativamente, è anche possibile modificare il **gruppo padre**. Per impostazione predefinita, il gruppo padre è il gruppo selezionato dall'utente nella fase di creazione del nuovo gruppo statico. Fare clic su **Fine** per creare il nuovo Gruppo statico.



6.1.1.6.2 Gestisci gruppi statici

Accedere ad **Amministrazione** > **Gruppi** e selezionare il Gruppo statico che si desidera gestire. Fare clic sul pulsante **Gruppo** o sulla rotella ⚙ accanto al nome del Gruppo statico. Verrà visualizzato un menu popup con le opzioni a disposizione:



Nuovo gruppo statico
Il Gruppo statico selezionato dopo aver fatto clic sul pulsante **Gruppo** o sulla rotella ⚙ sarà il gruppo padre predefinito ma è possibile modificare il gruppo padre più avanti (se necessario) quando si crea un nuovo gruppo statico.

Modifica gruppo
Consente all'utente di modificare il gruppo selezionato. Le stesse impostazioni valgono per la creazione di un nuovo gruppo (statico o dinamico).

Sposta
Consente all'utente di spostare il gruppo selezionato su un altro gruppo. Il gruppo spostato diventerà un sottogruppo di tale gruppo.

Elimina
Rimuove completamente il gruppo selezionato.

Esporta
Esporta i membri del gruppo (e dei sottogruppi, se selezionati) in un elenco (file *.txt*). Questo elenco può essere utilizzato per scopi di revisione oppure importato in un momento successivo.

Importa
È possibile importare un elenco (solitamente un file di testo) di computer come membri del gruppo selezionato.

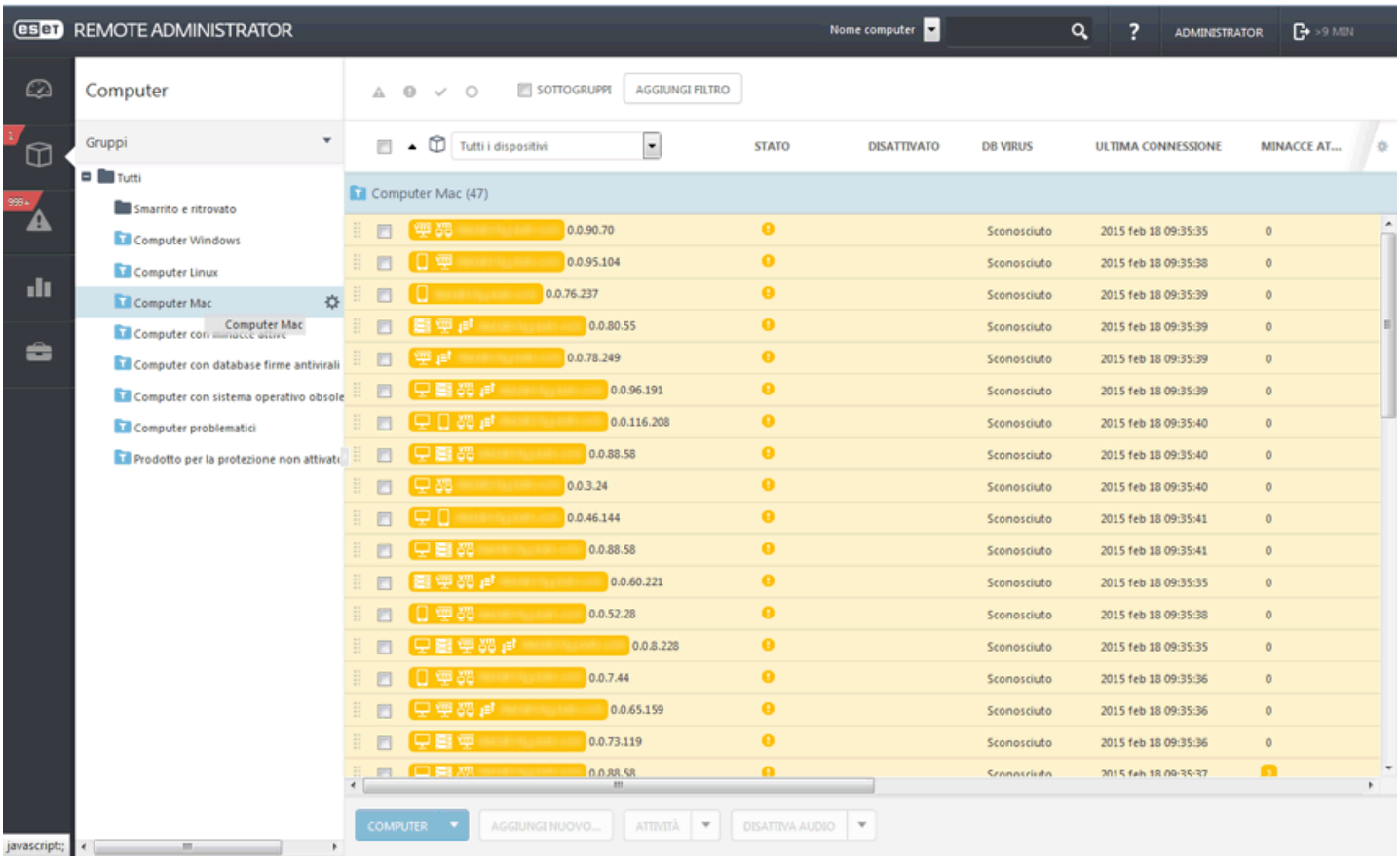
6.1.1.6.3 Sposta gruppo statico

Fare clic sul simbolo della rotella ⚙ accanto al nome del gruppo e selezionare **Sposta**. Verrà visualizzata una finestra popup contenente la struttura dei gruppi. Selezionare il gruppo di destinazione (statico o dinamico) nel quale si desidera spostare il gruppo selezionato. Il gruppo di destinazione diventerà un gruppo padre. È anche possibile spostare i gruppi trascinando e rilasciando un gruppo nel gruppo di destinazione desiderato.

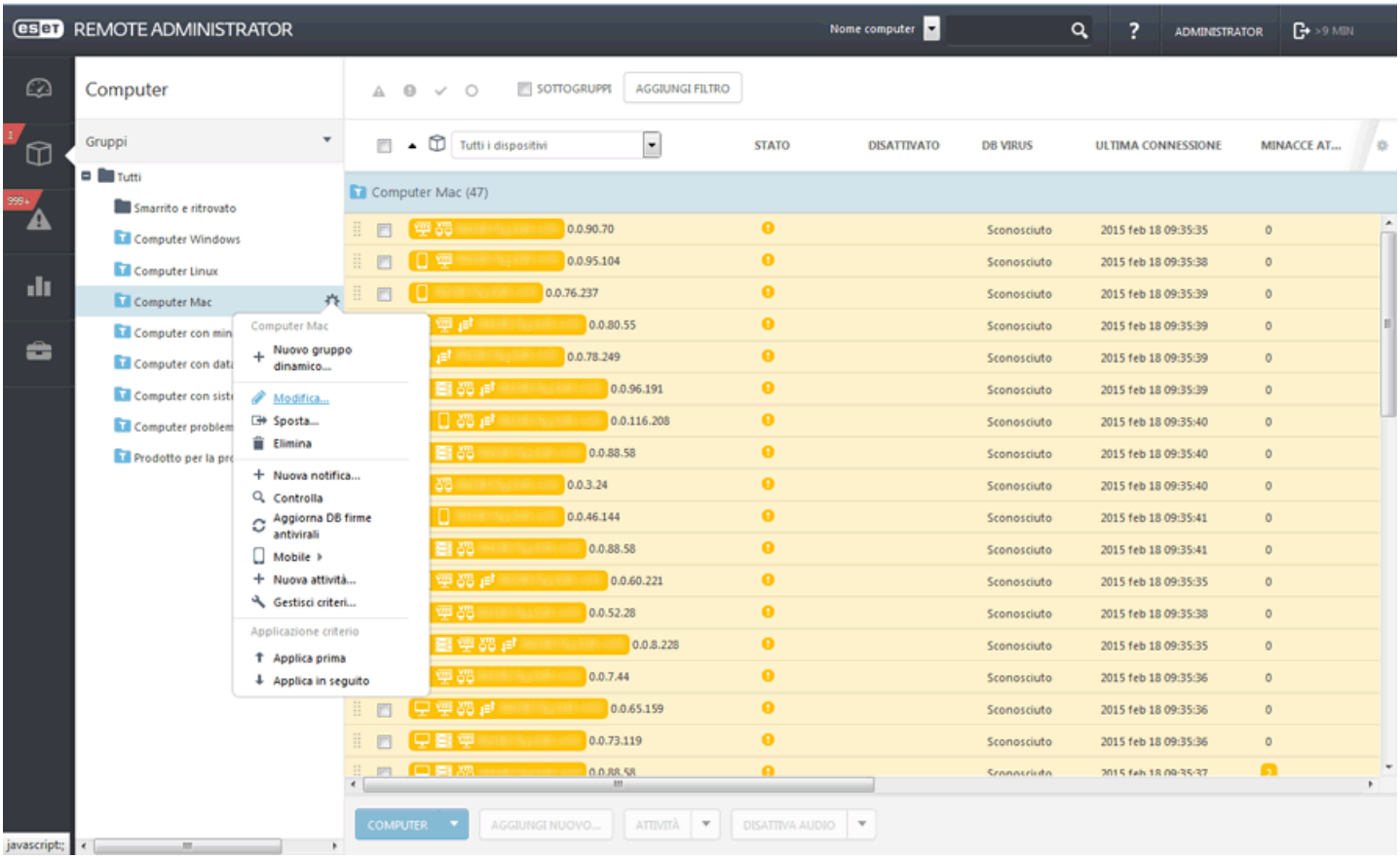
Si tengano presenti alcune eccezioni all'organizzazione dei gruppi. **Non è possibile spostare un gruppo statico in un gruppo dinamico**. Inoltre, non è possibile spostare Gruppi statici predefiniti (ad esempio Smarrito e ritrovato) in qualsiasi altro gruppo. È possibile spostare liberamente gli altri gruppi. Un Gruppo dinamico può essere membro di qualsiasi altro gruppo, compresi i Gruppi statici.

Per spostare i gruppi è possibile utilizzare i seguenti metodi:

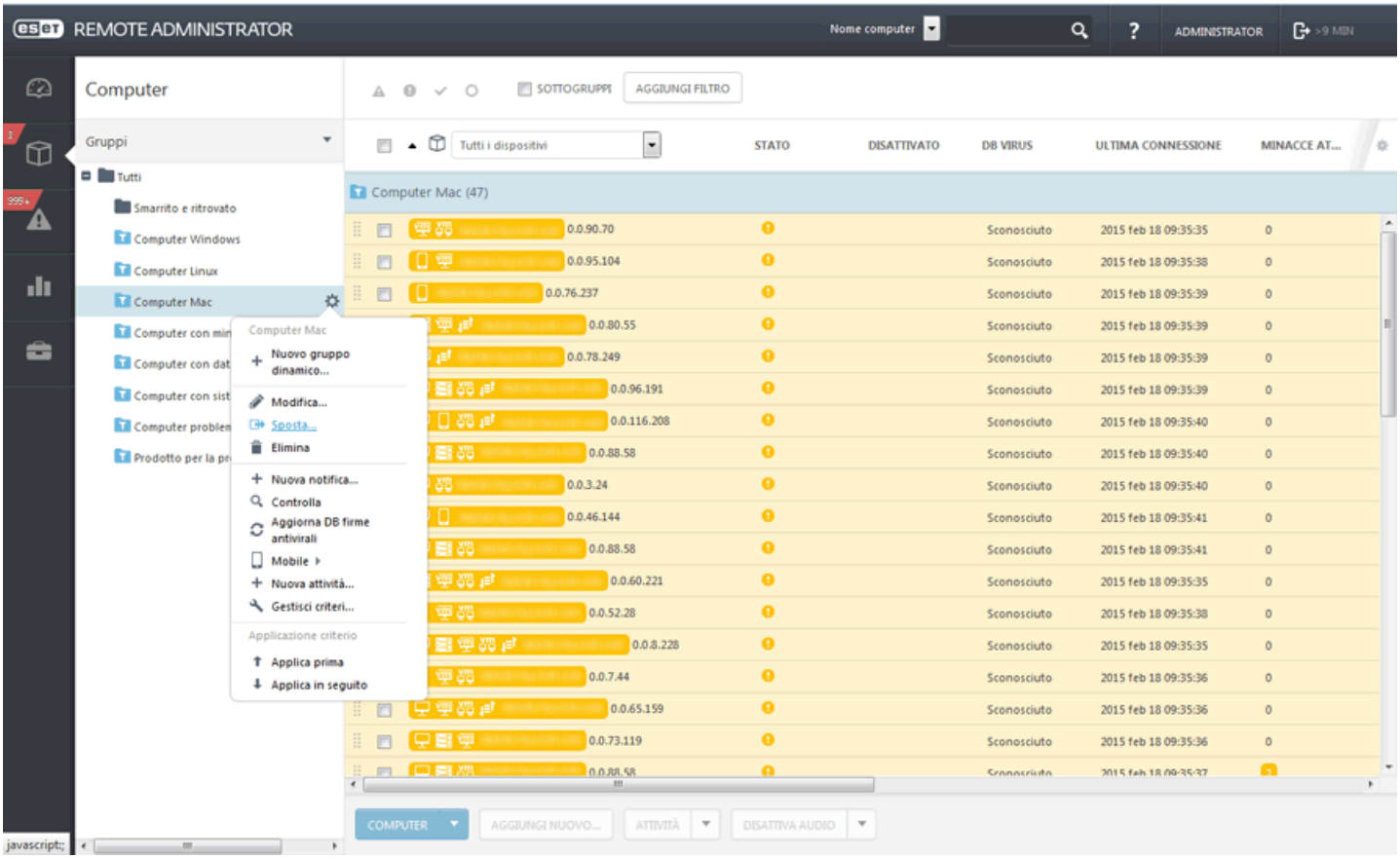
Trascina e rilascia: fare clic e trascinare il gruppo che si desidera spostare, quindi rilasciarlo sopra il nuovo gruppo padre.



⚙ > **Modifica** > **Modifica gruppo padre**.



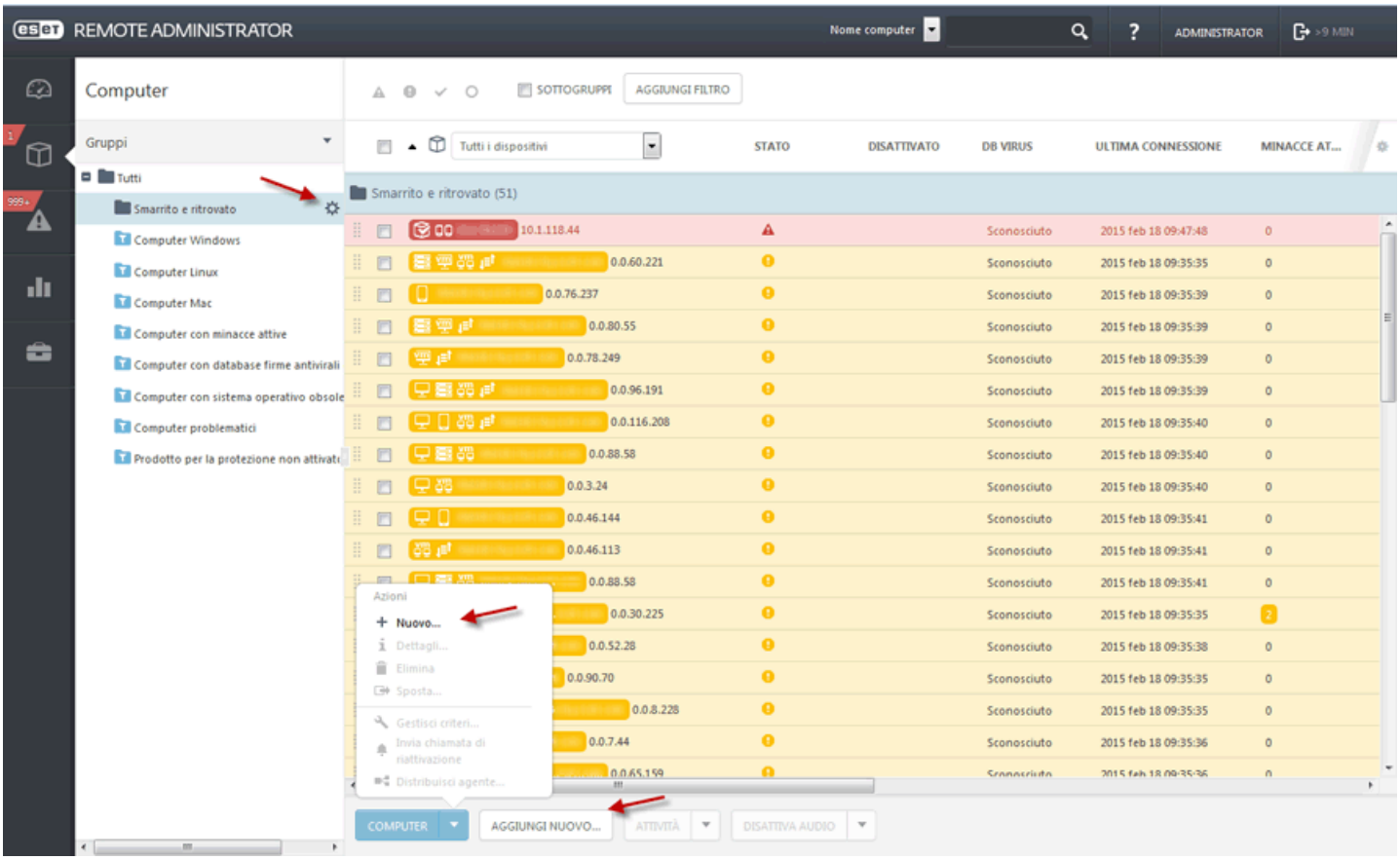
> **Sposta** > selezionare un nuovo gruppo padre dall'elenco e fare clic su **OK**.



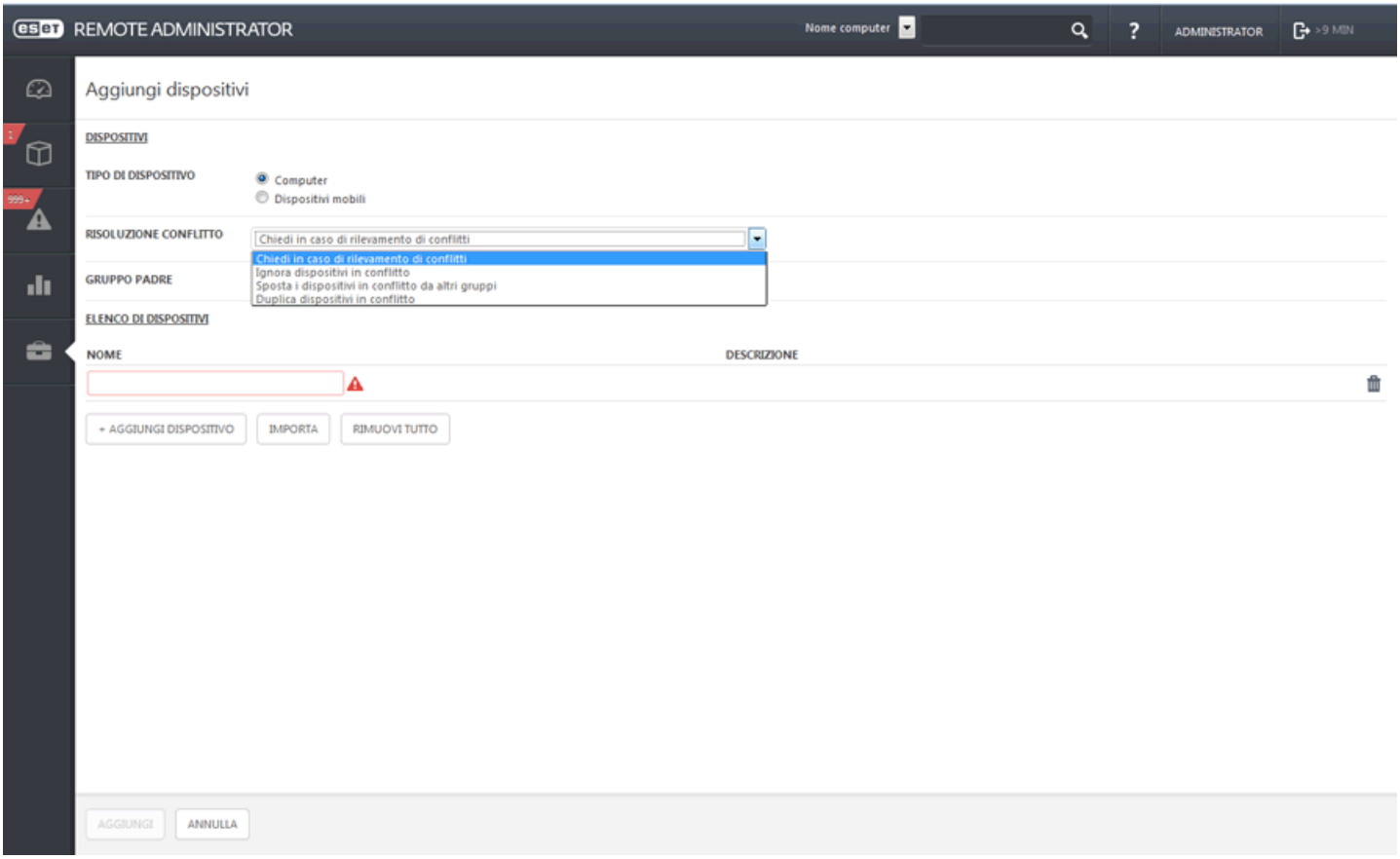
6.1.1.6.4 Aggiungi computer client a gruppo statico

Creare un nuovo gruppo statico o selezionare uno dei gruppi statici predefiniti.

Nella **scheda** Computer è possibile aggiungere nuovi computer in base a tre diverse modalità. Ad esempio, selezionare un gruppo statico: fare clic sull'icona a forma di rotella e selezionare **+ Aggiungi nuovo**.



Immettere il nome del computer che si desidera aggiungere nel campo **Nome**. Fare clic su + Aggiungi dispositivo per aggiungere altri computer oppure su Importa per importare un file contenente un elenco di computer da aggiungere. Facoltativamente, inserire una **descrizione** dei computer.



Utilizzare il menu a discesa Risoluzione conflitto per selezionare l'azione da eseguire se un computer che si sta aggiungendo esiste già in ERA:

Chiedi in caso di rilevamento di conflitti: in caso di rilevamento di un conflitto, il programma chiederà all'utente di selezionare un'azione (vedere le opzioni sottostanti).
Ignora computer in conflitto: I computer duplicati non verranno aggiunti.
Sposta i computer in conflitto da altri gruppi: i computer in conflitto verranno spostati dai gruppi originali al gruppo **Tutti**.
Duplica computer in conflitto: verranno aggiunti nuovi computer, ma con nomi diversi.

Fare clic su **Aggiungi**. È possibile visualizzare i computer nell'elenco sulla destra dopo aver selezionato il relativo gruppo di appartenenza.

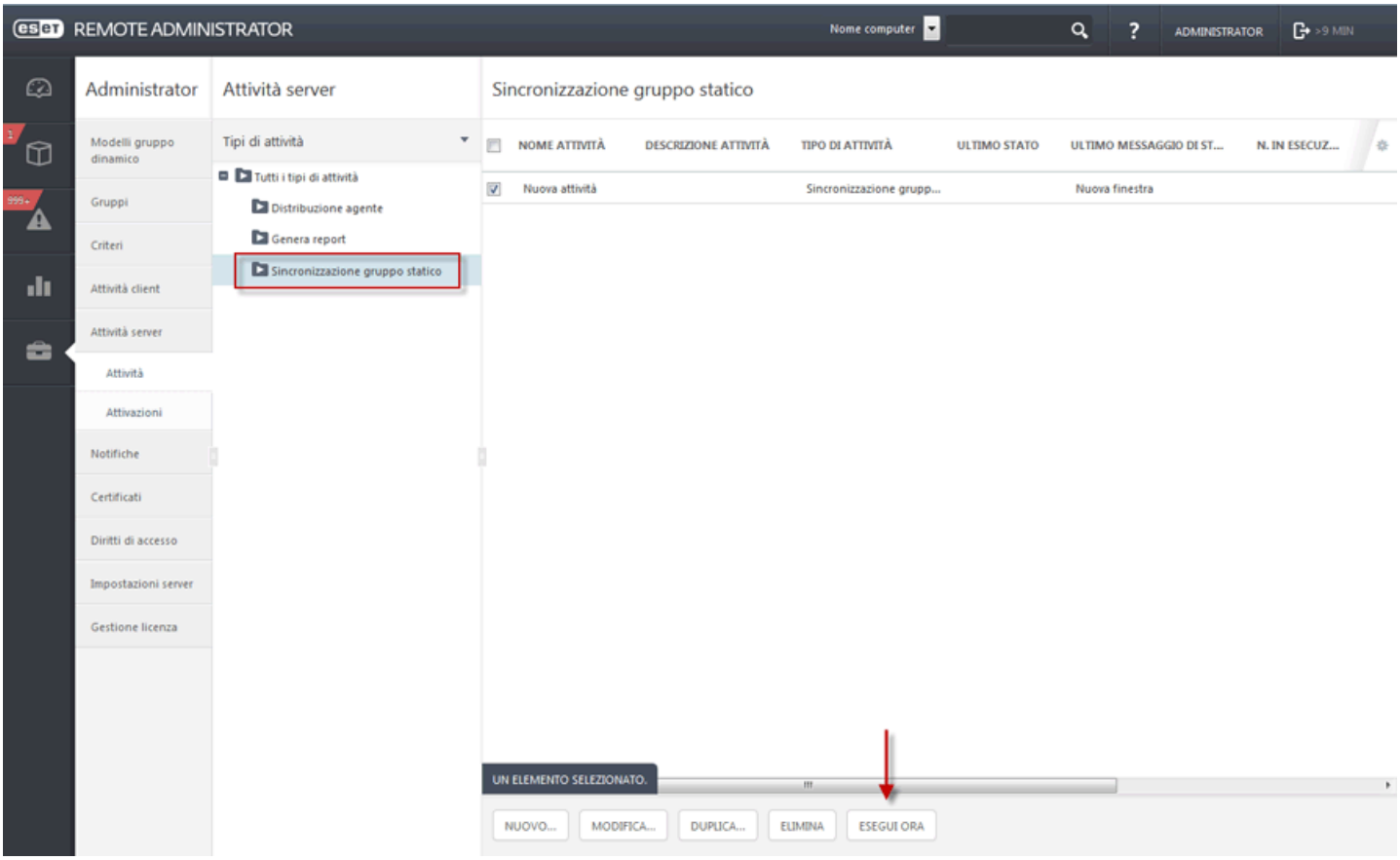
NOTA: l'aggiunta di computer multipli potrebbe richiedere più tempo. Potrebbe essere eseguita una ricerca DNS inversa.

Per ulteriori informazioni sulle modalità di aggiunta dei dispositivi mobili, consultare il capitolo Registrazione dispositivi mobili.

6.1.1.6.5 Importa client da Active Directory

La sincronizzazione AD viene eseguita attraverso il lancio dell'attività del server **Sincronizzazione dei gruppi statici**.

Amministrazione > **Attività server** è un'attività predefinita preimpostata che è possibile scegliere di eseguire automaticamente durante l'installazione di ESET Remote Administrator. Se il computer si trova in un dominio, verrà eseguita la sincronizzazione e i computer provenienti da AD verranno inseriti nel gruppo predefinito **Tutti**.



Per avviare il processo di sincronizzazione, basterà fare clic sull'attività e scegliere **Esegui ora**. Se è necessario creare una nuova attività di sincronizzazione AD, selezionare il gruppo al quale aggiungere nuovi computer da AD. Scegliere inoltre gli oggetti nell'AD per i quali eseguire la sincronizzazione e quale azione eseguire per i duplicati. Immettere le impostazioni di connessione del server AD e impostare la **Modalità di sincronizzazione** su **Active Directory/Open Directory/LDAP**.

Seguire le istruzioni dettagliate contenute in questo articolo della Knowledge Base ESET.

6.1.1.6.6 Assegna un'attività a un gruppo statico

I Gruppi dinamici e statici sono trattati in maniera analoga per quanto riguarda l'assegnazione delle attività. Per informazioni sulle modalità di assegnazione di un'attività a un gruppo, fare clic qui.

6.1.1.6.7 Assegna un criterio a un gruppo statico

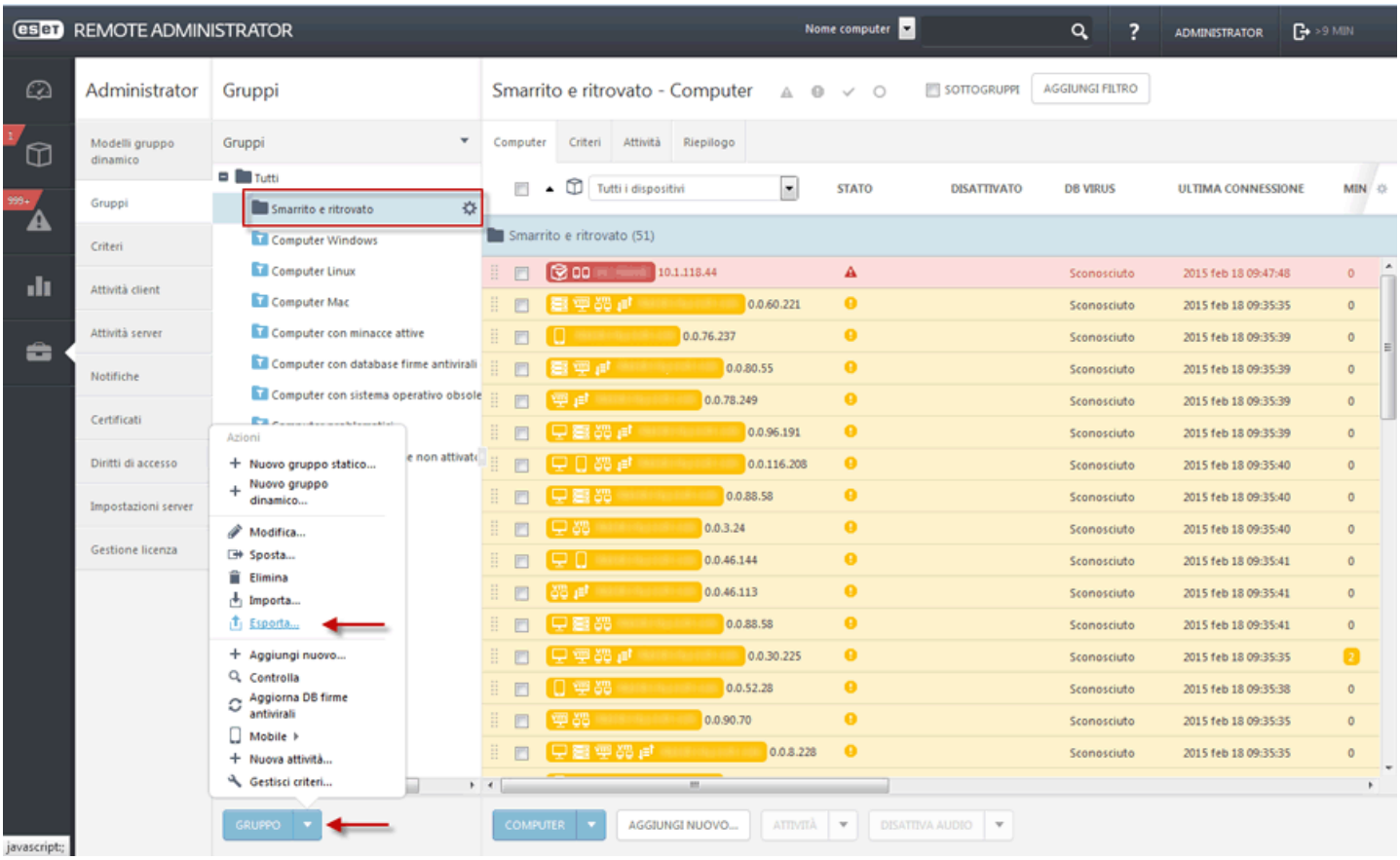
I Gruppi dinamici e statici sono trattati in maniera analoga per quanto riguarda l'assegnazione dei criteri. Per informazioni sulle modalità di assegnazione di un criterio a un gruppo, fare clic qui.

6.1.1.6.8 Esporta gruppi statici

L'esportazione di un elenco di computer presenti nella struttura ERA è un'operazione semplice. È possibile esportare l'elenco e archiviarlo come copia di backup in modo da poterlo importare nuovamente in futuro se si desidera, ad esempio, ripristinare la struttura del gruppo.

NOTA: i gruppi statici devono contenere almeno un computer. Non è possibile esportare gruppi vuoti.

1. Accedere ad **Amministrazione** > **Gruppi** > e selezionare il Gruppo statico che si desidera esportare.

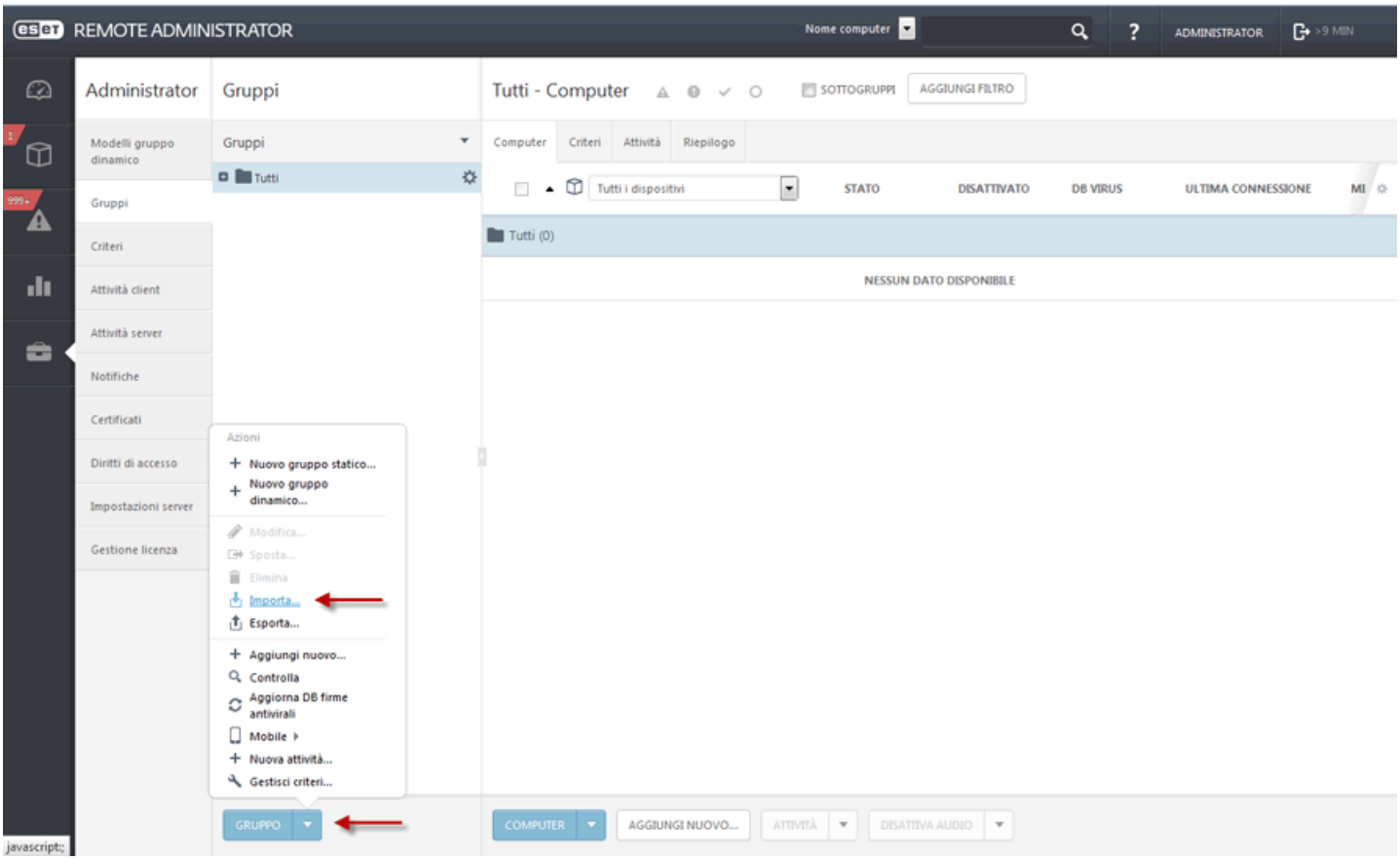


2. Fare clic sul pulsante **Gruppo** nella parte inferiore della pagina (comparirà un menu contestuale).
3. Selezionare **Esporta.**
4. Il file verrà salvato in formato **.txt**.

NOTA: i gruppi dinamici non possono essere esportati in quanto rappresentano solo collegamenti a computer in base ai criteri definiti nei modelli dei gruppi dinamici.

6.1.1.6.9 Importa gruppi statici

I file esportati dai gruppi statici possono essere importati nuovamente in ERA Web Console e inclusi nella struttura del gruppo esistente.



1. Fare clic su **Gruppo** (comparirà un menu contestuale).
2. Selezionare **Importa**.
3. Fare clic su **Sfoglia** e accedere al file **.txt**.
4. Selezionare il file del gruppo e fare clic su **Apri.** Il nome del file verrà visualizzato nella casella di testo.
5. Selezionare una delle seguenti opzioni per risolvere i conflitti:

- **Ignora computer in conflitto**

Se i Gruppi statici sono esistenti e i computer indicati nel file .txt sono già presenti nel gruppo, questi verranno ignorati e non verranno importati. Compariranno le informazioni su questa condizione.

- **Sposta i computer in conflitto da altri gruppi**

Se i Gruppi statici sono esistenti e i computer indicati nel file .txt sono già presenti nel gruppo, è necessario spostare i computer in altri Gruppi statici prima dell'importazione. Dopo questa operazione, i computer verranno spostati nuovamente nei gruppi originali dai quali sono stati prelevati.

- **Duplica computer in conflitto**

Se i gruppi statici sono esistenti e i computer indicati nel file .txt sono già presenti nel gruppo, verranno creati duplicati di questi computer nello stesso gruppo statico. Il computer originale verrà visualizzato insieme alle informazioni complete e il duplicato comparirà esclusivamente con il relativo nome.

5. Fare clic su **Importa** per importare i Gruppi statici e i computer presenti al loro interno.

6.1.1.7 Gruppi dinamici

I Gruppi dinamici sono essenzialmente filtri personalizzati definiti nei Modelli. I computer vengono filtrati sul lato dell'agente. Pertanto, non è necessario trasferire ulteriori informazioni sul server. L'agente decide in maniera autonoma a quali Gruppi dinamici appartiene un client e lo segnala al server. I Gruppi dinamici hanno le proprie regole definite nel Modello gruppo dinamico.

Dopo aver installato ESET Remote Administrator sono disponibili alcuni Gruppi dinamici predefiniti. Se necessario, è possibile creare Gruppi dinamici personalizzati. In fase di creazione, è prima necessario creare un modello, quindi creare un gruppo dinamico.

In alternativa, è possibile creare un nuovo gruppo dinamico e un nuovo modello.

Da un modello è possibile creare più di un Gruppo dinamico.

Un utente può utilizzare i Gruppi dinamici in altre parti di ERA. È possibile assegnare criteri o preparare un'attività per tutti i computer appartenenti ai Gruppi dinamici.

I Gruppi dinamici possono contenere Gruppi statici o Gruppi dinamici. Il gruppo di livello superiore è tuttavia sempre statico.

Tutti i Gruppi dinamici sotto un determinato Gruppo statico filtrano solo i computer di tale Gruppo statico, indipendentemente dal livello in cui si trovano nella struttura. Inoltre, per i filtri dei Gruppi dinamici nidificati, un Gruppo dinamico a un livello più profondo filtra i risultati del gruppo superiore.

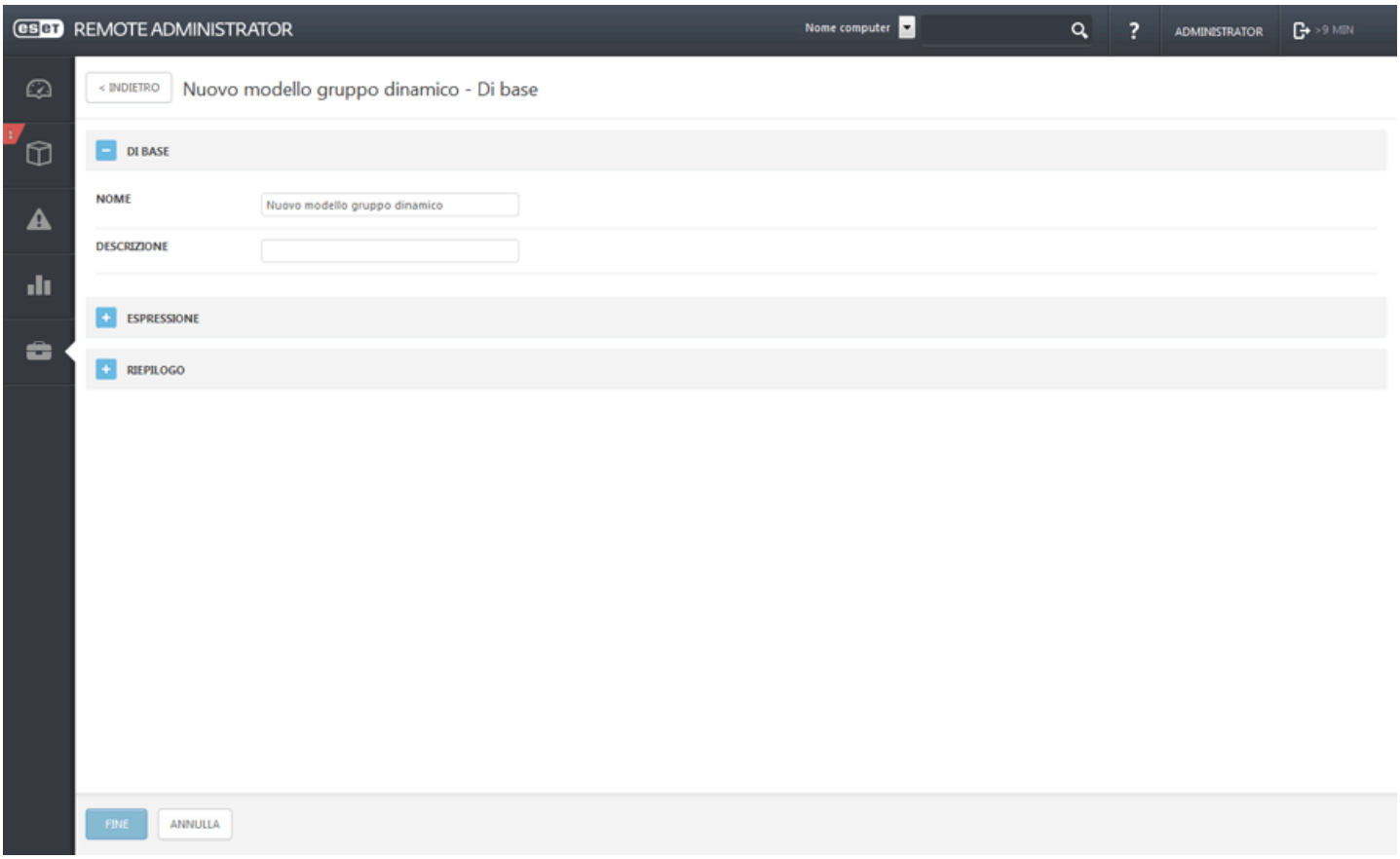
Tuttavia, una volta creati, possono essere spostati liberamente all'interno della struttura.

6.1.1.7.1 Procedura guidata modello gruppo dinamico

Fare clic su **Nuovo modello** in **Amministrazione** > **Modelli gruppi dinamici.**

Di base

1. Immettere un **Nome** e una **Descrizione** per il nuovo modello gruppo dinamico.



Espressione

Selezionare un operatore logico nel menu **Operazione**.

- **E**: tutte le condizioni definite devono essere vere.
- **O**: almeno una condizione deve essere vera.
- **NON E**: almeno una condizione deve essere falsa.
- **NON O**: tutte le condizioni devono essere false.

Ad esempio, selezionare **E**. Ciò significa che un computer deve soddisfare tutte le condizioni per poter apparire in un Gruppo dinamico che utilizza questo modello.

- Fare clic su **+ Aggiungi regola** e selezionare una condizione. ad esempio per i client che utilizzano i computer portatili collegati alla rete elettrica. Selezionare **Hardware** > **Alimentazione a batteria** > **=(uguale)** > **Non in esaurimento**.
- Fare clic su **+ Aggiungi regola** per immettere una seconda condizione (il numero di regole non è limitato). Selezionare **Edizione sistema operativo** > **Tipo di sistema operativo** > **=(uguale)** > **Windows 8.1** (immettere questo valore nel campo vuoto).

Se entrambe le suddette condizioni sono soddisfatte, il client apparirà nel Gruppo dinamico.

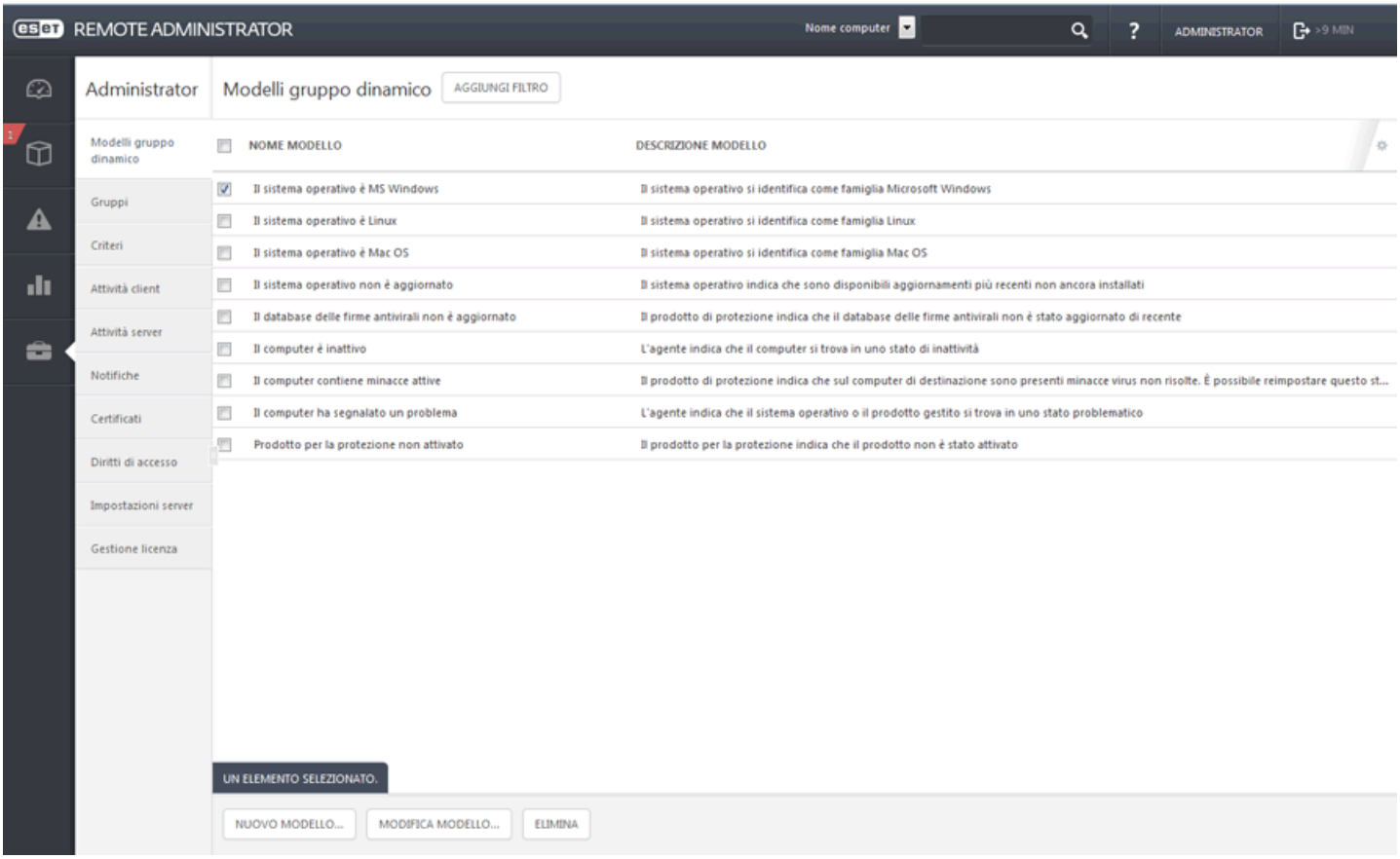
Riepilogo

Rivedere le impostazioni configurate e fare clic su **Fine** per creare il modello. Il nuovo modello verrà aggiunto all'elenco di tutti i modelli e può essere utilizzato più avanti per creare un nuovo gruppo dinamico. Nelle opzioni **Espressione** è possibile configurare le regole/condizioni per il gruppo (l'editor regole è descritto qui). Ora ogni gruppo dinamico basato su questo modello valuterà tali regole.

Per salvare le modifiche, fare clic su **Fine**.

6.1.1.7.2 Gestisci modelli gruppi dinamici

I Modelli possono essere gestiti da **Amministrazione** > **Modelli gruppi dinamici**.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Modelli gruppo dinamico
AGGIUNGI FILTRO
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
NOME MODELLO
DESCRIZIONE MODELLO
Il sistema operativo è MS Windows
Il sistema operativo si identifica come famiglia Microsoft Windows
Il sistema operativo è Linux
Il sistema operativo si identifica come famiglia Linux
Il sistema operativo è Mac OS
Il sistema operativo si identifica come famiglia Mac OS
Il sistema operativo non è aggiornato
Il sistema operativo indica che sono disponibili aggiornamenti più recenti non ancora installati
Il database delle firme antivirali non è aggiornato
Il prodotto di protezione indica che il database delle firme antivirali non è stato aggiornato di recente
Il computer è inattivo
L'agente indica che il computer si trova in uno stato di inattività
Il computer contiene minacce attive
Il prodotto di protezione indica che sul computer di destinazione sono presenti minacce virus non risolte. È possibile reimpostare questo st...
Il computer ha segnalato un problema
L'agente indica che il sistema operativo o il prodotto gestito si trova in uno stato problematico
Prodotto per la protezione non attivato
Il prodotto per la protezione indica che il prodotto non è stato attivato
UN ELEMENTO SELEZIONATO.
NUOVO MODELLO...
MODIFICA MODELLO...
ELIMINA

È possibile creare un Nuovo modello oppure modificare uno qualsiasi dei modelli esistenti. Fare clic sul modello che si desidera modificare per visualizzare una procedura guidata. In alternativa, è possibile selezionare un modello facendo clic sulla casella di controllo adiacente e selezionando quindi **Modifica modello**.

Espressione

Selezionare un operatore logico nel menu **Operazione**.

- **E**: tutte le condizioni definite devono essere vere.
- **O**: almeno una condizione deve essere vera.
- **NON E**: almeno una condizione deve essere falsa.
- **NON O**: tutte le condizioni devono essere false.

Ad esempio, selezionare **E**. Ciò significa che un computer deve soddisfare tutte le condizioni per poter apparire in un Gruppo dinamico che utilizza questo modello.

- Fare clic su **+ Aggiungi regola** e selezionare una condizione. ad esempio per i client che utilizzano i computer portatili collegati alla rete elettrica. Selezionare **Hardware** > **Alimentazione a batteria** > **=(uguale)** > **Non in esaurimento**.
- Fare clic su **+ Aggiungi regola** per immettere una seconda condizione (il numero di regole non è limitato). Selezionare **Edizione sistema operativo** > **Tipo di sistema operativo** > **=(uguale)** > **Windows 8.1** (immettere questo valore nel campo vuoto).

Se entrambe le suddette condizioni sono soddisfatte, il client apparirà nel Gruppo dinamico.

Riepilogo

Rivedere le impostazioni configurate e fare clic su **Fine** per creare il modello. Il nuovo modello verrà aggiunto all'elenco di tutti i modelli e può essere utilizzato più avanti per creare un nuovo gruppo dinamico. Nelle opzioni **Espressione** è possibile configurare le regole/condizioni per il gruppo (l'editor regole è descritto qui). Ora ogni gruppo dinamico basato su questo modello valuterà tali regole.

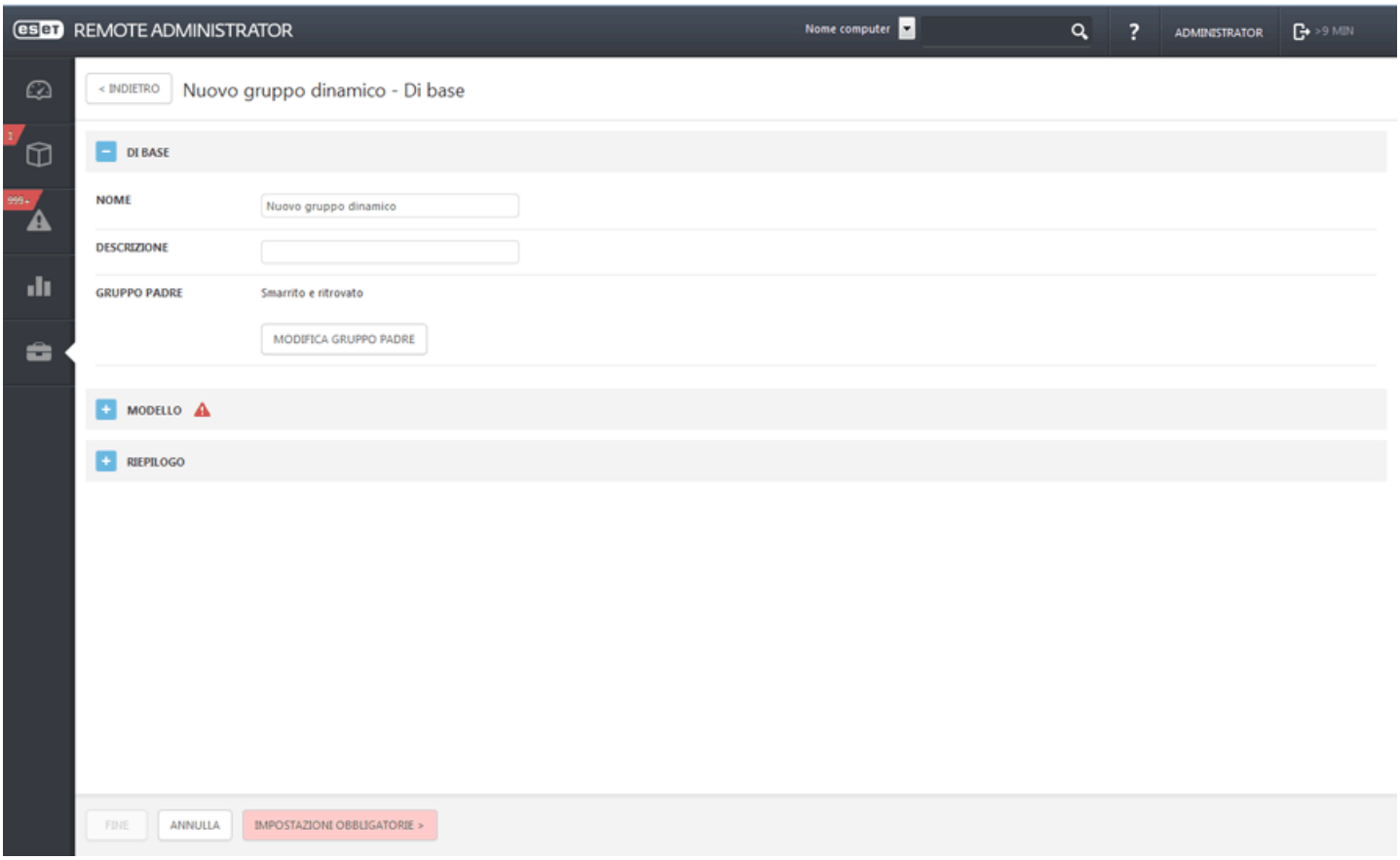
Per salvare le modifiche, fare clic su **Fine**.

6.1.1.7.3 Procedura guidata gruppo dinamico

È possibile creare Gruppi dinamici tramite un modello esistente o un nuovo modello (che verrà quindi utilizzato per tale Gruppo dinamico).

Di base

Immettere un **Nome** e una **Descrizione** (facoltativa) per il nuovo Gruppo dinamico. Per impostazione predefinita, il gruppo padre è il gruppo selezionato dall'utente nella fase iniziale della creazione del nuovo gruppo statico. Per modificare il gruppo padre, fare clic su **Modifica gruppo padre** e selezionarne uno dalla struttura. Il padre del nuovo gruppo dinamico può essere dinamico o statico. Fare clic su **Fine** per creare il nuovo gruppo dinamico.



Modello

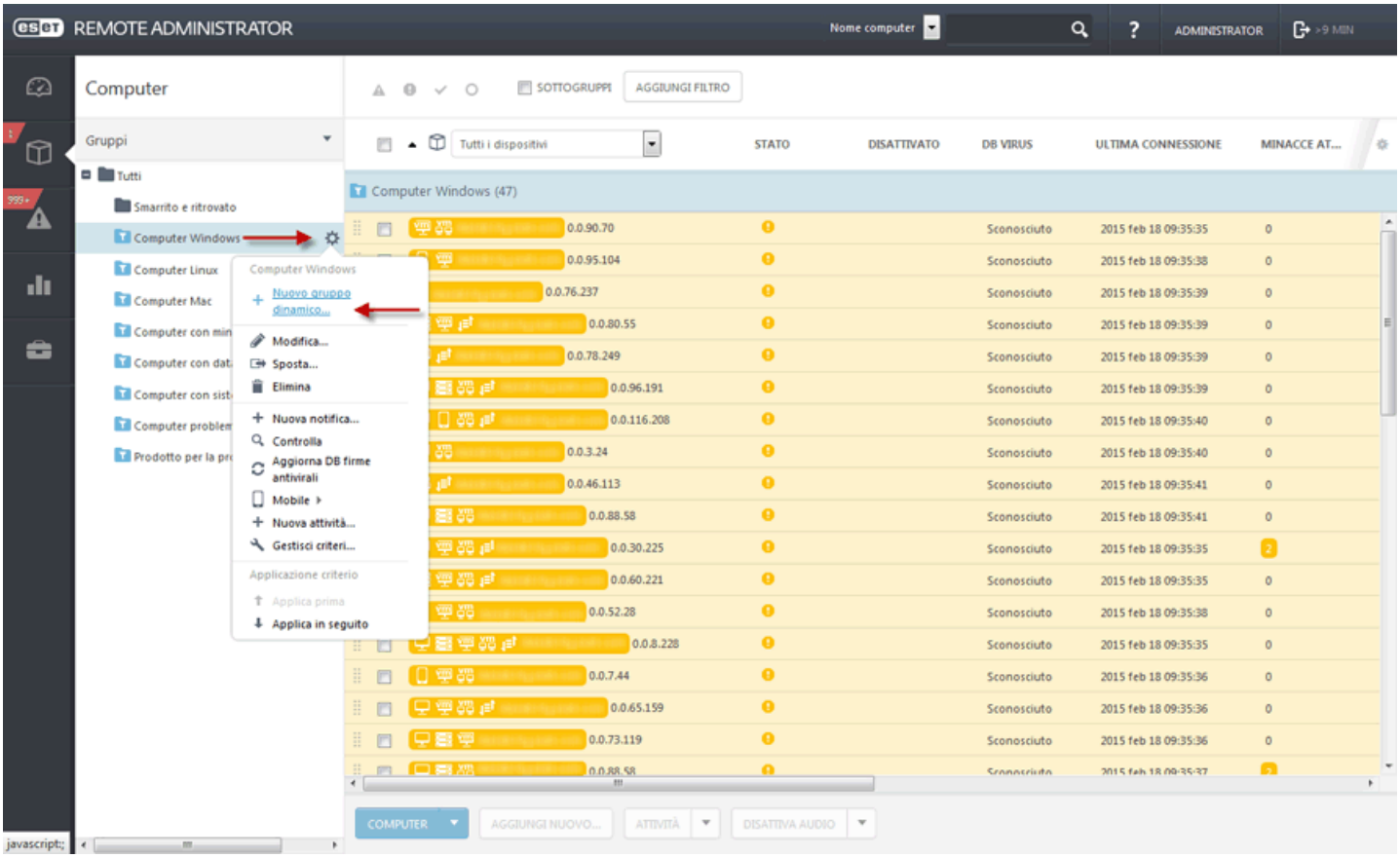
È possibile selezionare un modello gruppo dinamico esistente o creare un nuovo modello gruppo dinamico.

Riepilogo

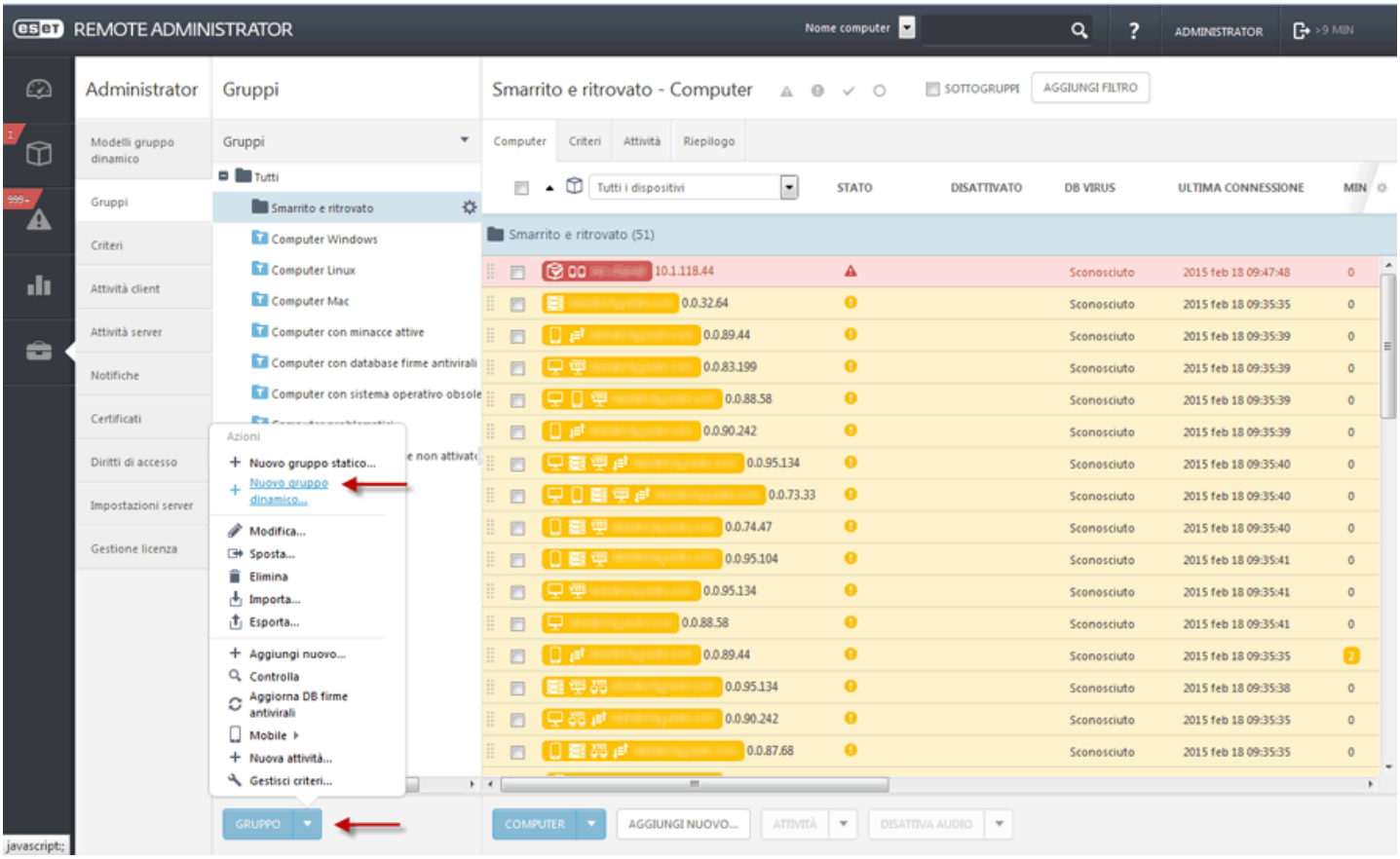
Controllare la configurazione per verificare che sia corretta (se necessario, è ancora possibile modificarla) e fare clic su **Fine**.

6.1.1.7.4 Crea gruppo dinamico tramite il modello esistente

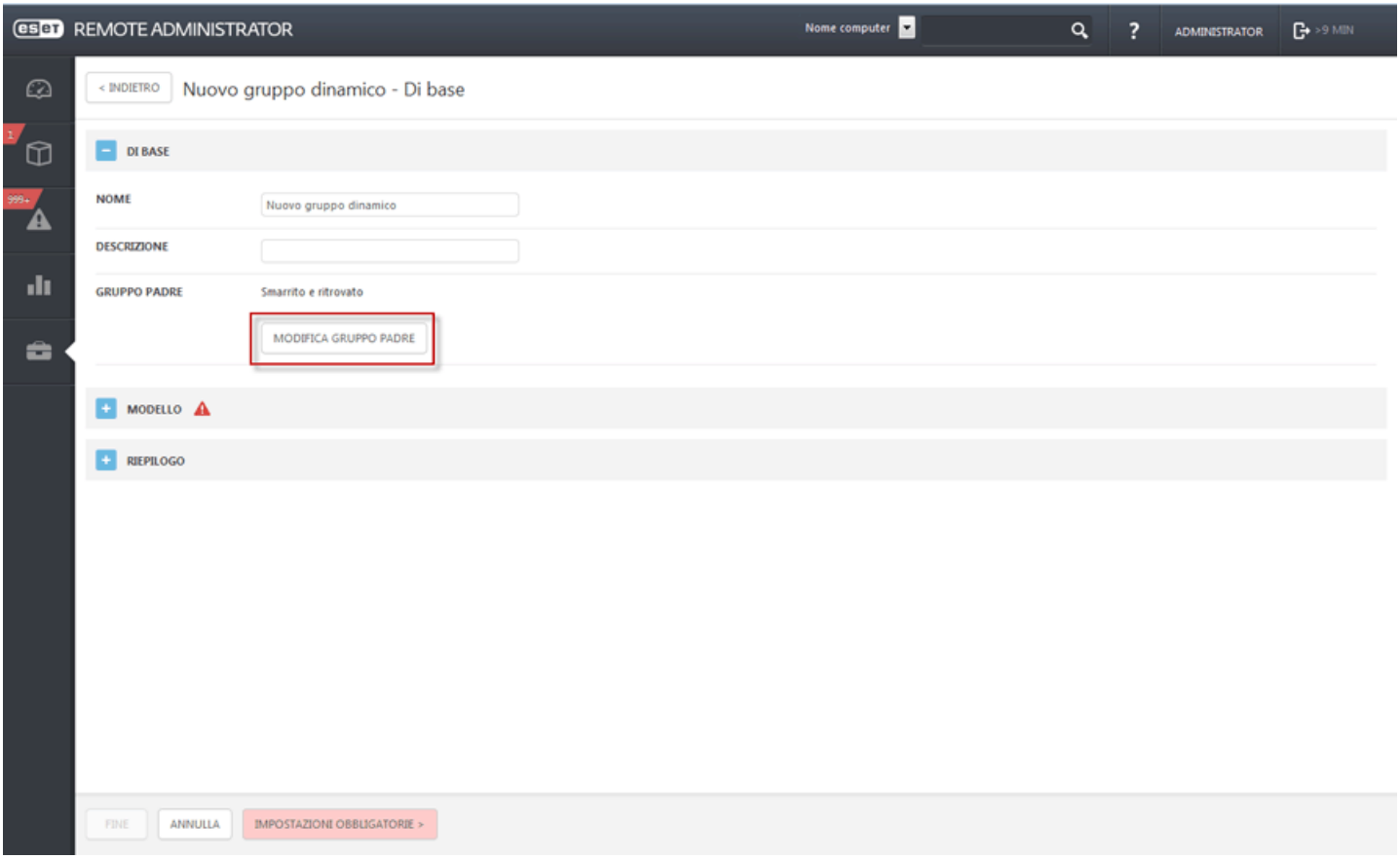
Per creare un nuovo Gruppo dinamico tramite un modello esistente, fare clic sul simbolo della rotella ⚙ accanto al nome del Gruppo dinamico, quindi fare clic su **Nuovo gruppo dinamico.**



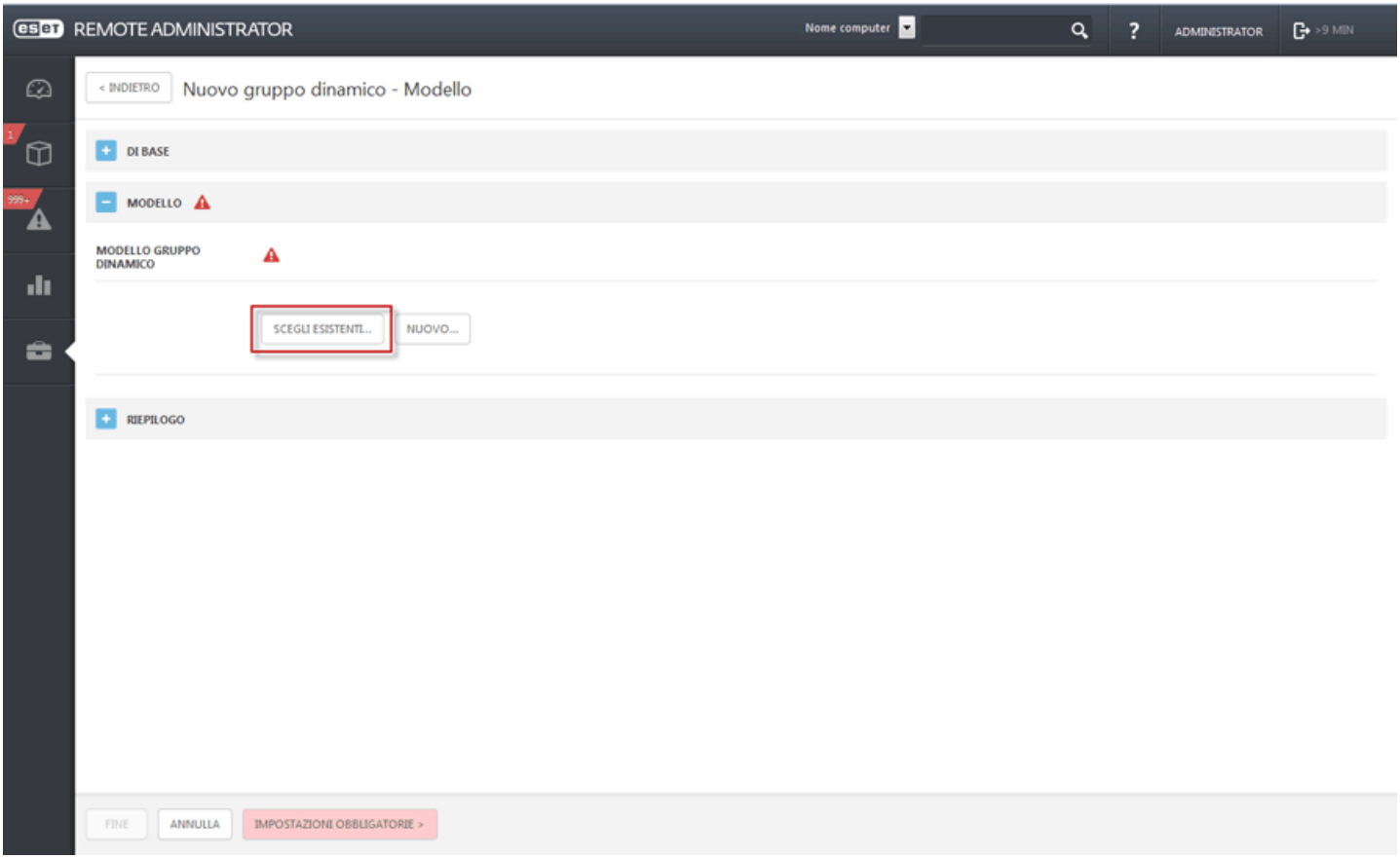
In alternativa, è possibile accedere all'opzione **Nuovo gruppo dinamico...** da **Amministrazione** > **Gruppi.** Selezionare un gruppo (nel riquadro Gruppi) e fare clic su **Gruppo** nella parte inferiore.



Verrà visualizzata una Procedura guidata gruppo dinamico. Immettere un **Nome** e una **Descrizione** (facoltativa) per il nuovo modello. È anche possibile modificare il gruppo padre facendo clic sul pulsante **Modifica gruppo padre**.



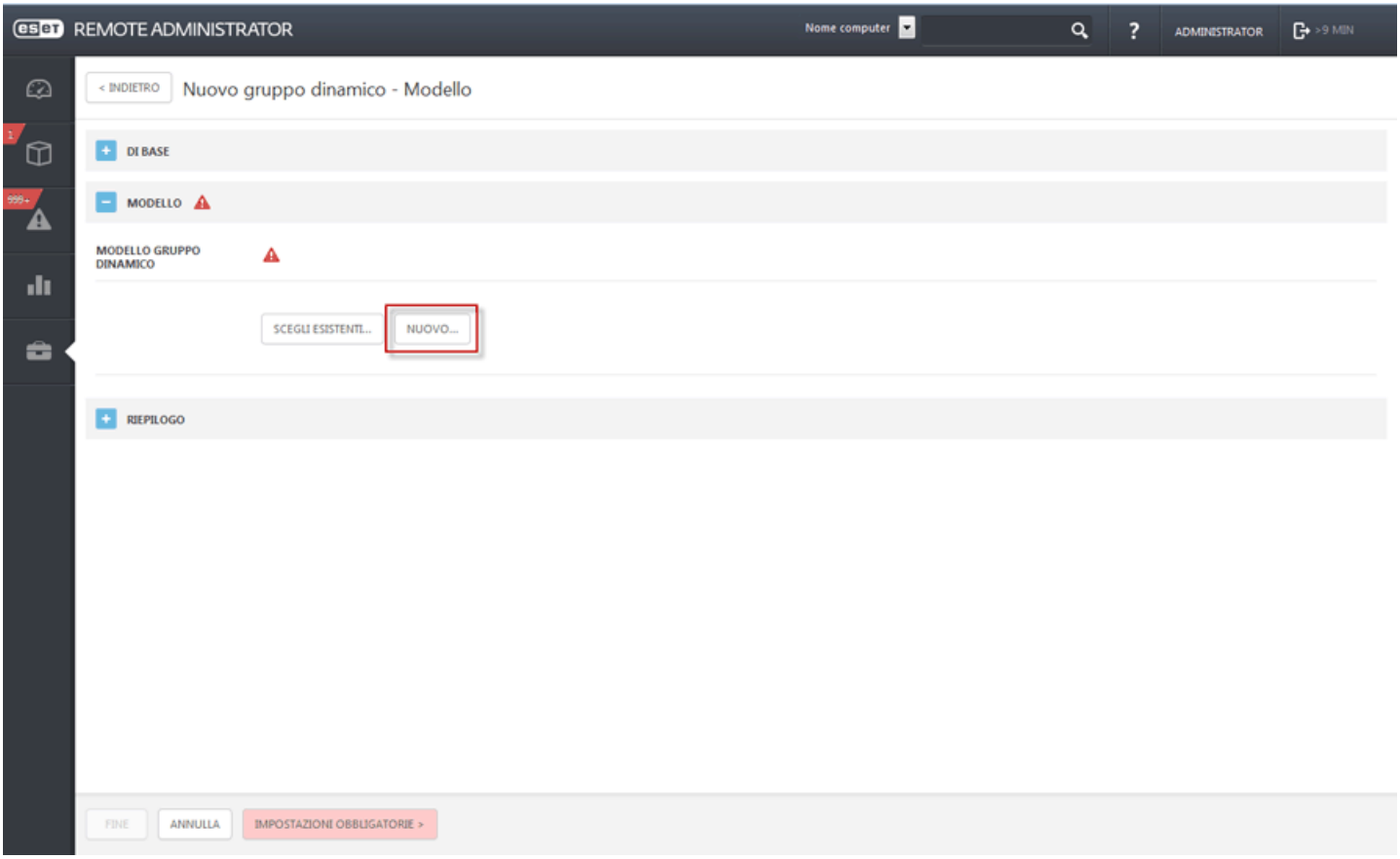
Selezionare **Modello gruppo dinamico** dai modelli predefiniti oppure scegliere uno di quelli già creati. Fare clic su **Scegli da esistenti** e scegliere il modello appropriato dall'elenco. Nel caso in cui non sia stato ancora creato alcun modello e nessuno di quelli predefiniti soddisfi le proprie esigenze, fare clic su Nuovo e seguire i passaggi per creare un nuovo modello.



Nell'ultima schermata viene visualizzato un riepilogo. Il nuovo gruppo viene visualizzato sotto il Gruppo statico padre.

6.1.1.7.5 Crea gruppo dinamico tramite nuovo modello

I passaggi sono analoghi a quelli utilizzati quando si crea un nuovo gruppo dinamico tramite un modello esistente fino al passaggio **Modello gruppo dinamico** dove si fa clic su Nuovo modello gruppo dinamico e si immettono le informazioni relative al nuovo modello.



Al termine, viene utilizzato automaticamente questo nuovo modello. Il modello verrà inoltre visualizzato nell'elenco Modelli gruppi dinamici e può essere utilizzato per creare altri Gruppi dinamici.

6.1.1.7.6 Gestisci gruppi dinamici

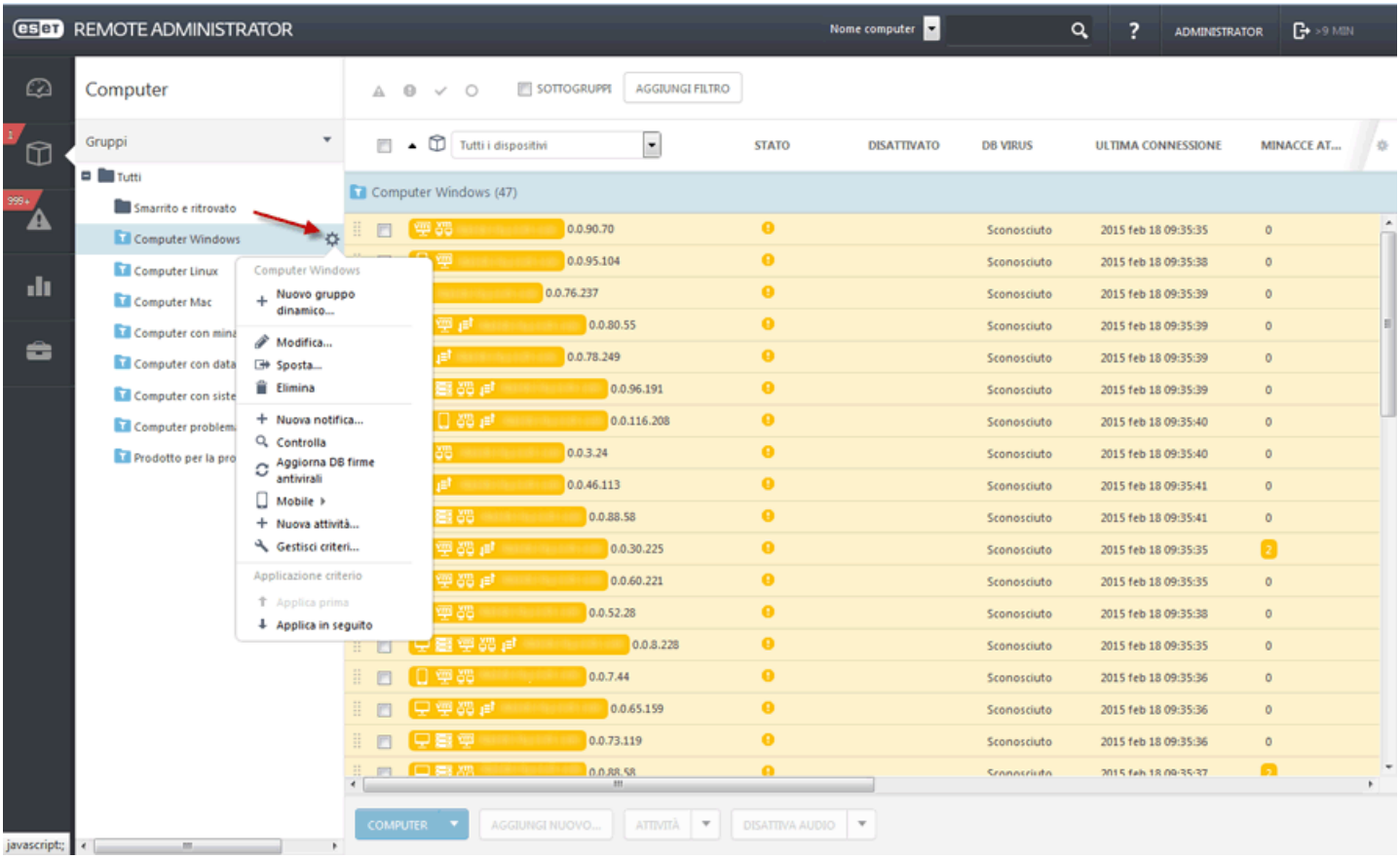
È possibile creare un Gruppo dinamico tramite un modello esistente o creare un nuovo modello che verrà utilizzato per tale Gruppo dinamico.

Una volta creato, su ogni Gruppo dinamico è possibile eseguire varie operazioni. quali

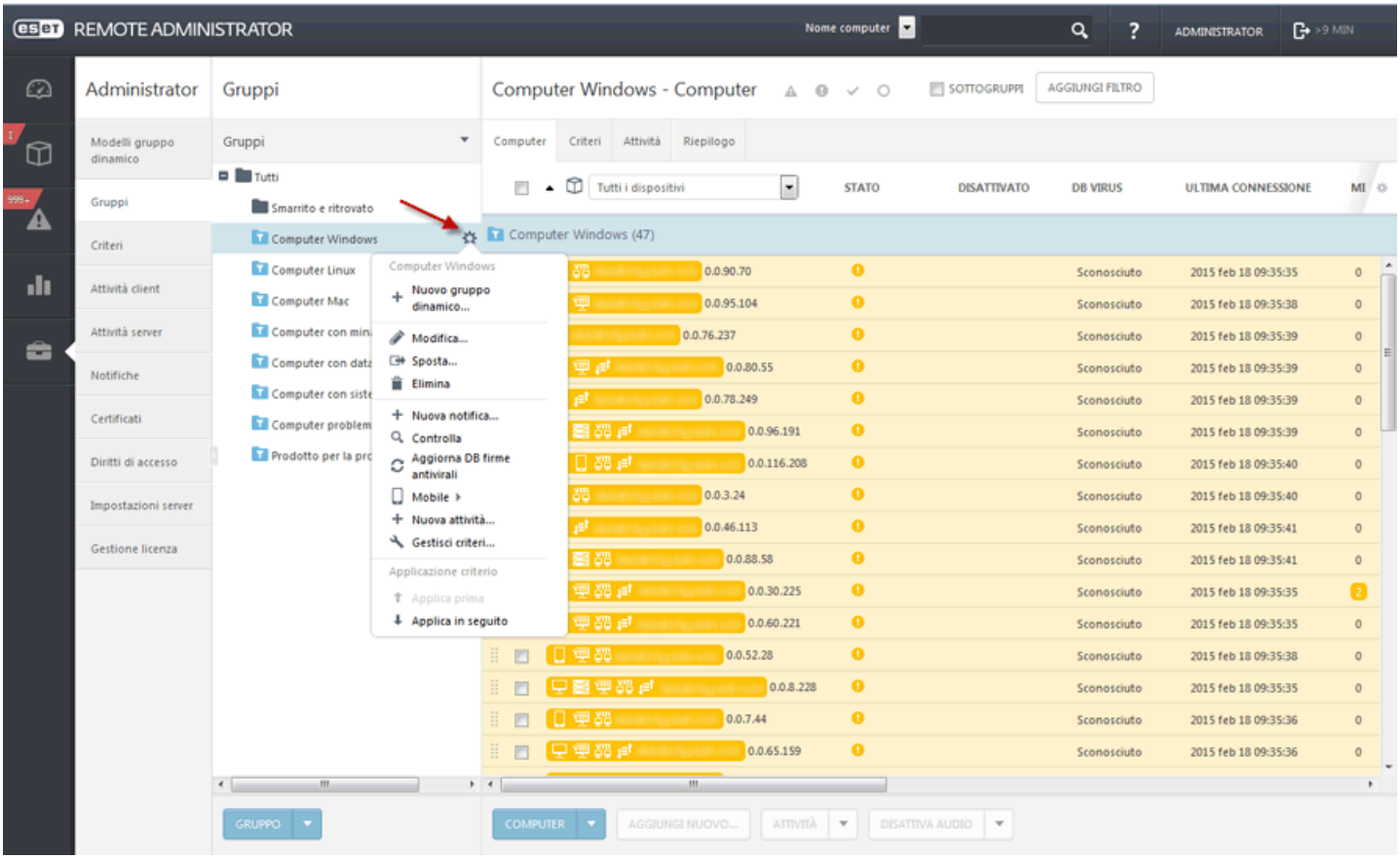
- Modifica
- Sposta
- Elimina
- Esegui attività
- Utilizza per le notifiche

Queste operazioni possono essere eseguite da tre percorsi:

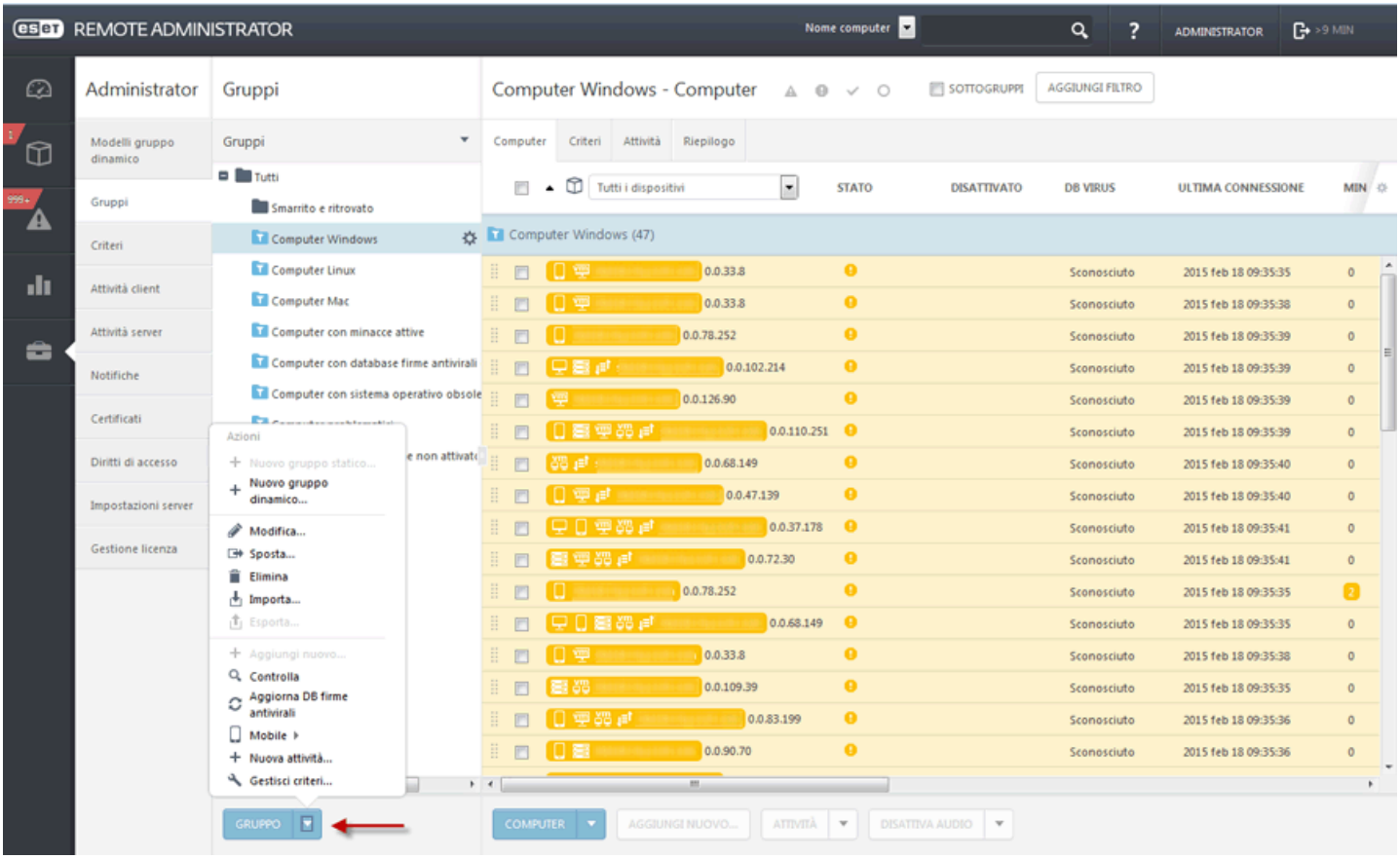
1. **Computer** > **Gruppi** > ⚙



2. **Amministrazione** > **Gruppi** > ⚙



3. **Amministrazione** > **Gruppi** > selezionare i Gruppi dinamici che si desidera gestire e fare clic su **Gruppo**.



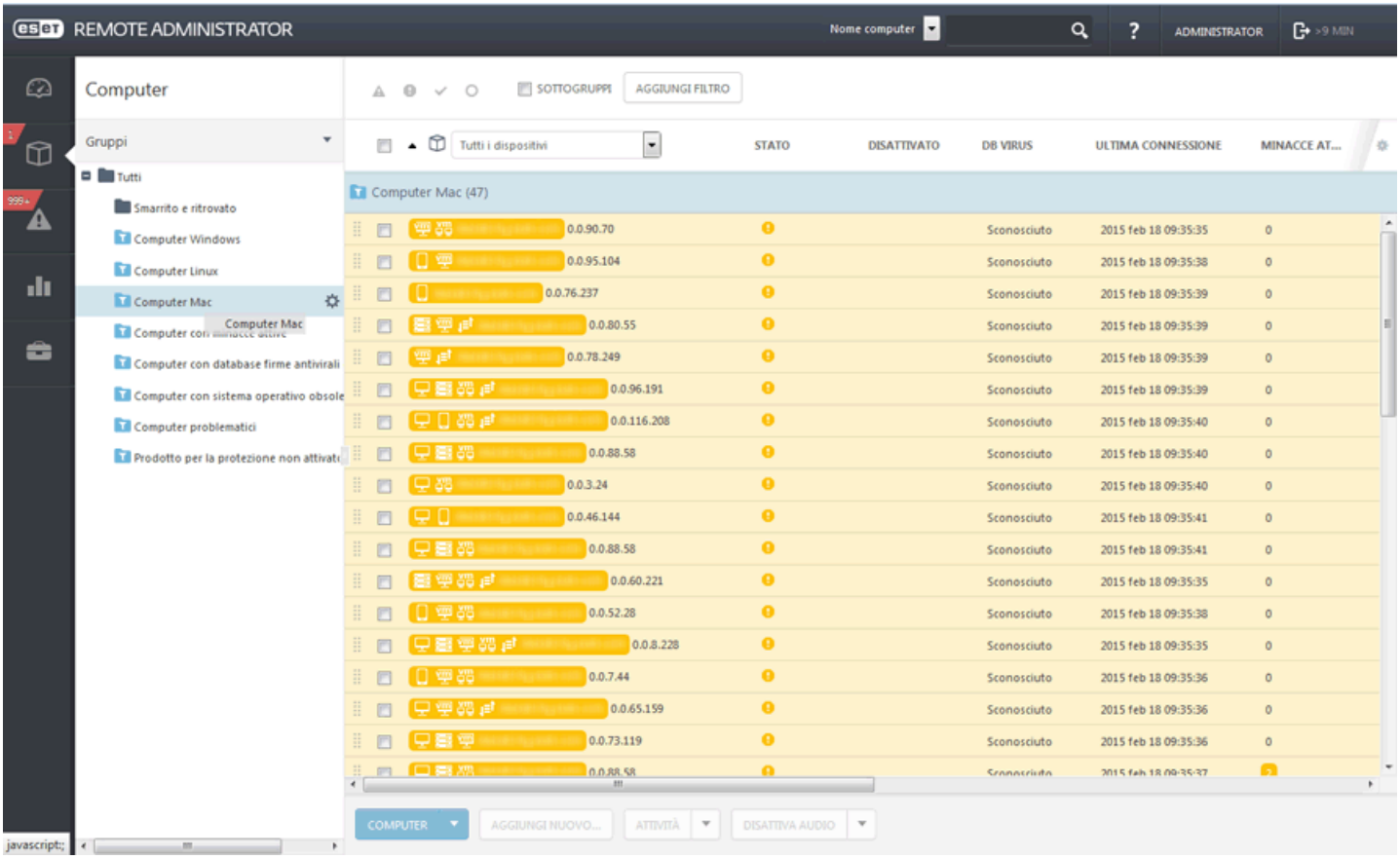
6.1.1.7.7 Sposta gruppo dinamico

Fare clic sul simbolo della rotella ⚙ accanto al nome del gruppo e selezionare **Sposta**. Verrà visualizzata una finestra popup contenente la struttura dei gruppi. Selezionare il gruppo di destinazione (statico o dinamico) nel quale si desidera spostare il gruppo selezionato. Il gruppo di destinazione diventerà un gruppo padre. È anche possibile spostare i gruppi trascinando e rilasciando un gruppo nel gruppo di destinazione desiderato.

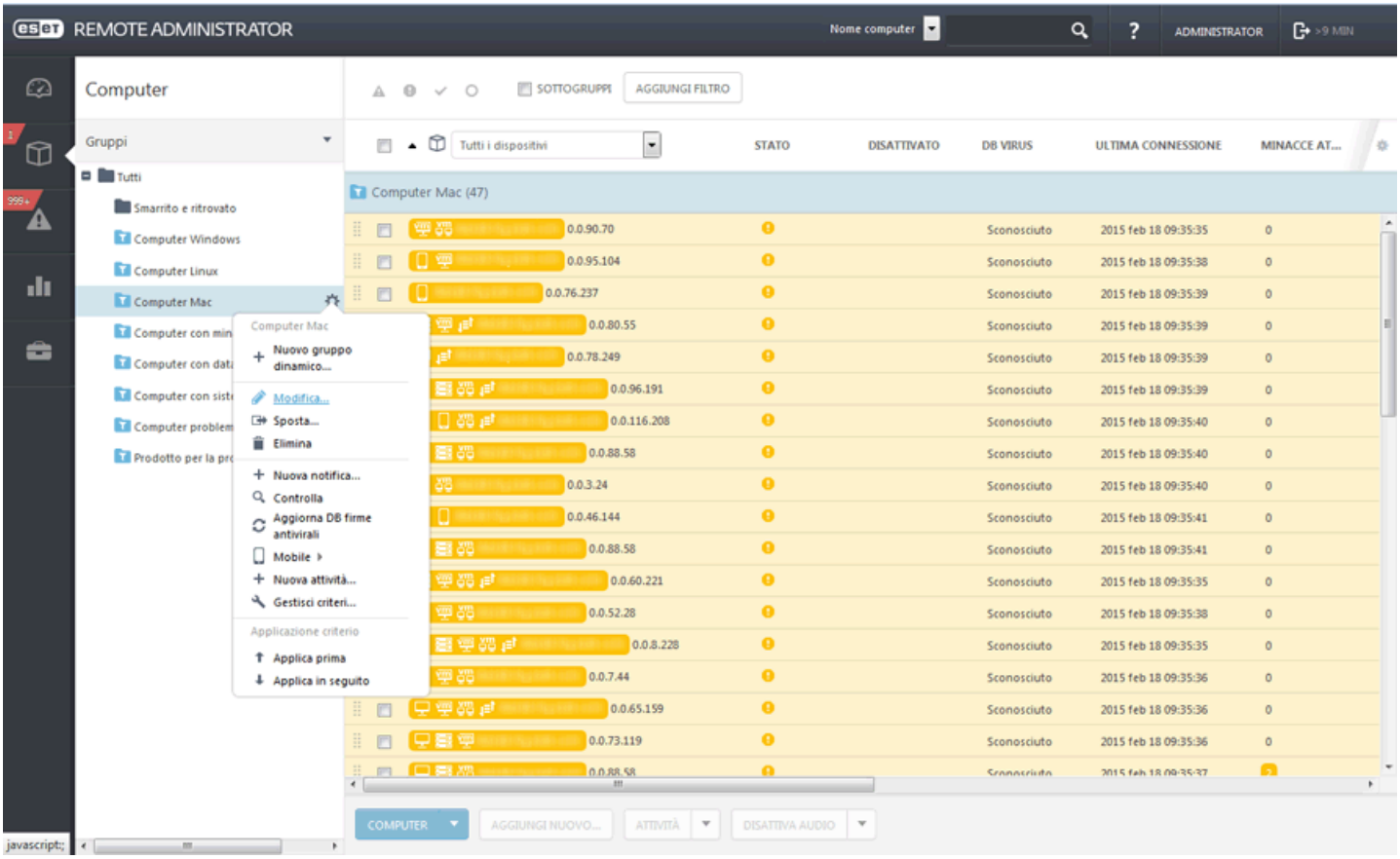
Si tengano presenti alcune eccezioni all'organizzazione dei gruppi. **Non è possibile spostare un gruppo statico in un gruppo dinamico**. Inoltre, non è possibile spostare Gruppi statici predefiniti (ad esempio Smarrito e ritrovato) in qualsiasi altro gruppo. È possibile spostare liberamente gli altri gruppi. Un Gruppo dinamico può essere membro di qualsiasi altro gruppo, compresi i Gruppi statici.

Per spostare i gruppi è possibile utilizzare i seguenti metodi:

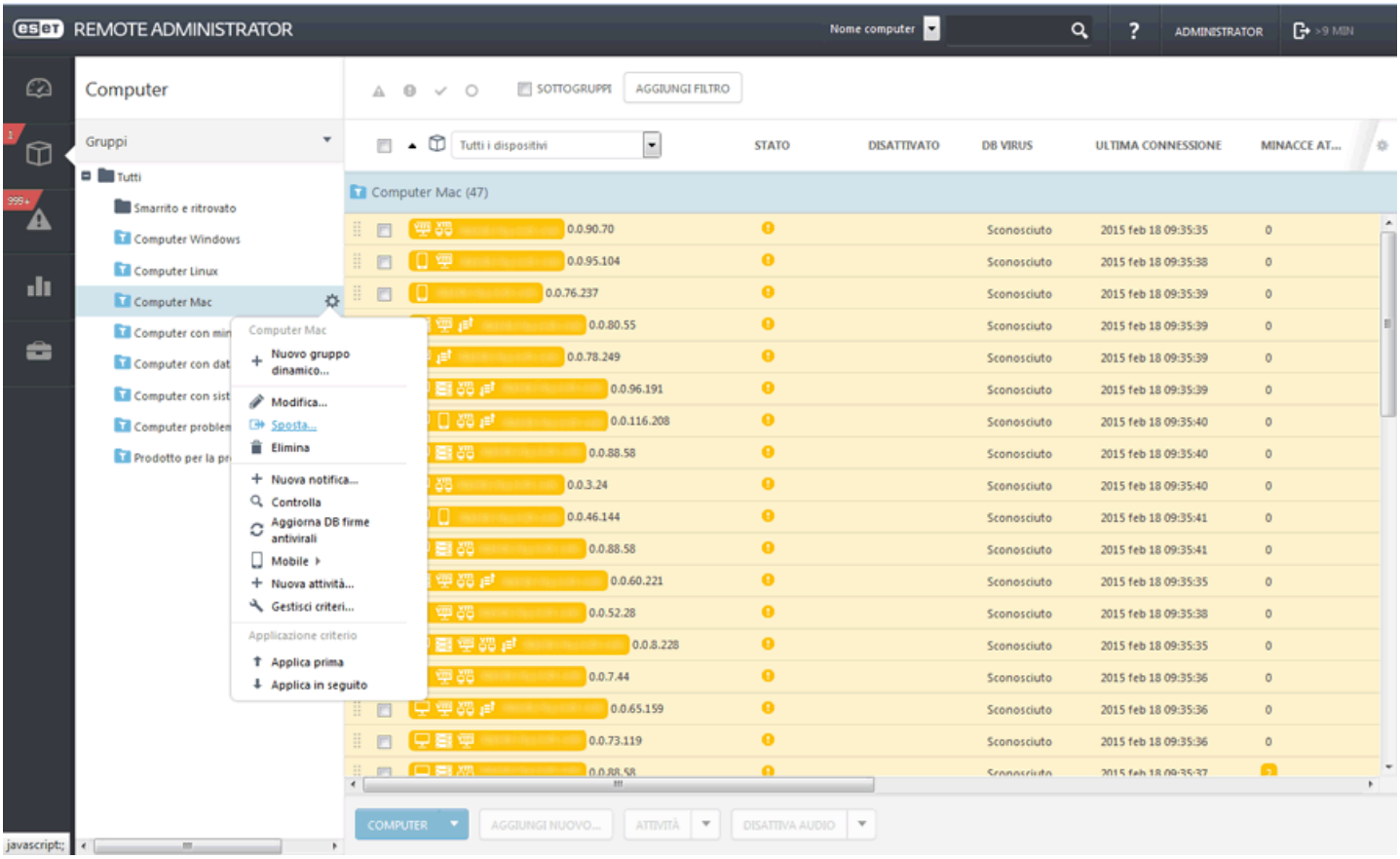
Trascina e rilascia: fare clic e trascinare il gruppo che si desidera spostare, quindi rilasciarlo sopra il nuovo gruppo padre.



> **Modifica** > **Modifica gruppo padre**.



> **Sposta** > selezionare un nuovo gruppo padre dall'elenco e fare clic su **OK**.



NOTA: il Gruppo dinamico in una nuova posizione inizia a filtrare i computer (in base al modello) senza alcuna relazione rispetto alla precedente posizione.

6.1.1.7.8 Assegna un criterio a un gruppo dinamico

I Gruppi dinamici e statici sono trattati in maniera analoga per quanto riguarda l'assegnazione dei criteri. Per informazioni sulle modalità di assegnazione di un criterio a un gruppo, fare clic qui.

6.1.1.7.9 Assegna un'attività a un gruppo dinamico

I Gruppi dinamici e statici sono trattati in maniera analoga per quanto riguarda l'assegnazione delle attività. Per informazioni sulle modalità di assegnazione di un'attività a un gruppo, fare clic qui.

6.1.1.7.10 Come automatizzare ESET Remote Administrator

1. Creare un gruppo dinamico, ad esempio: "Computer infetti"
2. Creare un'attività per il controllo approfondito e assegnarla a un gruppo dinamico Computer infetti (l'attività viene attivata quando i client entrano a far parte del Gruppo dinamico)
3. Creare un criterio specifico (in questo caso, "criterio di isolamento): quando è installato un prodotto di protezione ESET, creare una regola firewall che bloccherà tutto il traffico, ad eccezione della connessione a ESET Remote Administrator.
4. Creare un modello di notifica per i computer infetti (è possibile specificare varie condizioni): verrà attivata una notifica per segnalare all'utente la diffusione di una minaccia.

- Utilizzando la stessa tecnica è possibile automatizzare gli aggiornamenti dei prodotti e del sistema operativo, il controllo, le attivazioni automatiche di prodotti appena aggiunti con una licenza preselezionata e altre attività.

6.1.1.7.11 Quando un computer diventa un membro di un gruppo dinamico?

Affinché un computer possa diventare un membro di un particolare Gruppo dinamico, è necessario che soddisfi determinate condizioni. Tali condizioni sono definite in un Modello gruppo dinamico. Ciascun modello è costituito da una o più Regole (=Condizioni). Tali regole possono essere specificate in fase di creazione di un nuovo Modello.

Alcune informazioni sulla condizione corrente di un computer client sono archiviate presso l'agente. La condizione del computer viene quindi valutata dall'agente in base alle regole del Modello.

L'utente ERA potrebbe essere interessato solo a determinati stati. Definisce tale stato specificando i valori per stati specifici: questo insieme predefinito è noto come Gruppo dinamico.

Non appena qualsiasi macchina entra nello stato di tali valori specifici, viene assegnata automaticamente a questo gruppo.

I Gruppi dinamici possono essere considerati come filtri basati sullo stato del computer. Un computer può corrispondere a più di un filtro e, pertanto, essere assegnato a più di un Gruppo dinamico. Ciò differenzia i Gruppi dinamici da quelli statici dove un computer può risiedere solo una volta.

6.1.1.7.12 Valutazione delle regole del modello

La valutazione delle regole del modello è gestita dall'agente, non dal server ERA (a cui verrà inviato solo il risultato). Il processo di valutazione viene eseguito in base alle regole che sono configurate in un modello. Di seguito viene riportata una spiegazione del processo di valutazione insieme ad alcuni esempi.

Lo stato è un gruppo di varie informazioni. Alcune fonti forniscono più di uno stato dimensionale per macchina (ad esempio Sistema operativo, Dimensioni RAM, ecc.), mentre altre forniscono informazioni sullo stato con dimensioni multiple (ad esempio, Indirizzo IP, Applicazione installata, ecc.).

Di seguito viene riportata una rappresentazione visiva dello stato di un client:

Schede di rete.Indirizzo IP	Schede di rete.Indirizzo MAC	Nome.SO	Versione.SO	Dimensioni HW.RAM in MB	Applicazione installata
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Lo stato è costituito da gruppi di informazioni. Un gruppo di dati fornisce informazioni coerenti organizzate in righe. Il numero di righe per gruppo può variare.

Le condizioni sono valutate per gruppo e per riga: se sono presenti più condizioni inerenti le colonne da un gruppo, vengono presi in considerazione solo i valori sulla stessa riga.

Esempio 1:

Ai fini di questo esempio si tenga conto della seguente condizione:

```
Schede di rete.Indirizzo IP = 10.1.1.11 AND Schede di rete.Indirizzo MAC = 4A-64-3F-10-FC-75
```

Questa regola non corrisponde ad alcun computer e non esiste alcuna riga dove entrambe le condizioni sono veritiere.

Schede di rete - Indirizzo IP	Schede di rete - Indirizzo MAC	Nome sistema operativo	Versione sistema operativo	Dimensioni HW - RAM in MB	Software installato
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Esempio 2:

Ai fini di questo esempio si tenga conto della seguente condizione:

```
Schede di rete.Indirizzo IP = 192.168.1.2 AND Schede di rete.Indirizzo MAC = 4A-64-3F-10-FC-75
```

Questa volta, entrambe le condizioni corrispondono a celle sulla stessa riga e, pertanto, la regole viene valutata nel suo insieme come VERITIERA. Viene selezionato un computer.

Schede di rete - Indirizzo IP	Schede di rete - Indirizzo MAC	Nome sistema operativo	Versione sistema operativo	Dimensioni HW - RAM in MB	Software installato
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Esempio 3:

Per condizioni con l'operatore OR (almeno una condizione deve essere VERITIERA), ad esempio:

```
Schede di rete.Indirizzo IP = 10.1.1.11 OR Schede di rete.Indirizzo MAC = 4A-64-3F-10-FC-75
```

la regola è VERITIERA per due righe, poiché deve essere soddisfatta solo una delle condizioni. Viene selezionato un computer.

Schede di rete - Indirizzo IP	Schede di rete - Indirizzo MAC	Nome sistema operativo	Versione sistema operativo	Dimensioni HW - RAM in MB	Software installato
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

6.1.1.7.13 Editor regole

Condizioni

Quando si impostano le condizioni per un modello Gruppo dinamico, esistono operatori differenti da utilizzare per le diverse condizioni.

Sono disponibili 3 tipi di elenchi:

- Gli elenchi operatori numerici contengono gli operatori che mettono a confronto i valori numerici
- Gli elenchi operatori di tipo stringa contengono gli operatori che mettono a confronto i valori alfanumerici
- Gli elenchi operatori booleani contengono solo due operatori true "= (uguale)" e false "≠ (non uguale)"

Tipi di elenchi operatore

L'elenco contiene 6 valori:

- "= (uguale)"
- "≠ (non uguale)"
- "> (maggiore di)"
- "≥ (maggiore o uguale)"
- "< (minore di)"
- "≤ (minore o uguale)"

Elenco operatori di tipo stringa

L'elenco contiene 9 valori:
- "= (uguale)": imposta solo il valore ricercato esatto e intero
- "≠ (non uguale)": imposta solo il valore esatto e intero che si desidera ignorare nella ricerca
- "contiene sottostringa": imposta una sottostringa in qualsiasi punto dell'espressione
- "contiene prefisso": imposta esattamente i primi caratteri della stringa di ricerca, ad es. nella stringa "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", il prefisso indica "Micros" o "Micr" o "Microsof" ecc.
- "contiene suffisso": imposta esattamente gli ultimi caratteri della stringa di ricerca, ad es. nella stringa "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", il suffisso indica "319" o "0.30319", ecc.
- "regex": utilizza una sintassi Perl
- "in": imposta un'espressione esatta, ad es. per la stringa "Microsoft Windows" è necessario scrivere esattamente "Microsoft Windows"
- "contiene maschera" e "in (maschera stringa)" contengono 2 tipi di caratteri jolly:
- *: corrispondente a qualsiasi numero di caratteri (0 o più)
- ?: corrispondente a 1 carattere esatto

Esempi

- "a*" corrisponde ad "a", "aa", "ax", "abcde"
- "a?" corrisponde ad "aa", "ab", "ac" ma non ad "a" o "aaa"
- "a??" corrisponde ad "aaa", "aab", "axy" ma non ad "a", "aa" o "aaaa"
- "a?*" corrisponde ad "aa", "ax", "abcde" ma non ad "a"
- "*a*" corrisponde ad "a", "xa", "ax", "xax", "dynamic", "abba"
- "?*" corrisponde a tutto tranne che a ""

Elenco operatori booleani

L'elenco contiene 2 valori che sono tuttavia sempre connessi all'elenco della seconda condizione:

- "= (uguale)": la condizione successiva è true
- "≠ (non uguale)": la condizione successiva è false

- Le operazioni matematiche di base (ad es. maggiore di) sono abbastanza autoesplicative. Per le altre operazioni, viene fornita una breve spiegazione:

operatore "contiene sottostringa". Vero se l'operando è una sottostringa del valore del simbolo.
operatore "contiene prefisso". Vero se il valore del simbolo inizia con il valore dell'operando, ad esempio, "xyz" contiene il prefisso "xy".
operatore "contiene suffisso". Vero se il valore del simbolo termina con il valore dell'operando, ad esempio, "xyz" contiene il suffisso "yz".
operatore "contiene maschera". Consente l'utilizzo dei caratteri jolly per il confronto delle stringhe, ad esempio, "*z" corrisponde a "xyz"
operatore "regex". Vero se il simbolo corrisponde al regex nell'operando. Viene utilizzata la sintassi Perl di regex.
operatore "in". L'operando è un elenco di valori. Vero se il valore del simbolo è uguale ad almeno uno dei valori dell'operando, ad esempio, "xyz" in ("abc", "def", "xyz").
operatore "in (maschera stringa)". L'operando è un elenco di valori che consentono i caratteri jolly. Vero se il valore del simbolo corrisponde ad almeno uno dei valori dell'operando, ad esempio, "xyz" in ("a*", "*f", "*z").
operatore "non ha valore". Vero se il simbolo non ha valore. Il secondo operando viene ignorato.
operatore "ha valore". Vero se il simbolo ha un valore. Il secondo operando viene ignorato.

6.1.2 Criteri

I criteri vengono utilizzati per forzare specifiche configurazioni sui prodotti ESET in esecuzione sui computer client. Questo consente all'utente di evitare di configurare manualmente il prodotto ESET di ciascun client. Un criterio può essere applicato direttamente a singoli Computer oltre che a gruppi (statici e dinamici). È inoltre possibile assegnare più criteri a un computer o a un gruppo, diversamente dai criteri in ESET Remote Administrator 5 e versioni precedenti dove era possibile applicare un criterio a un prodotto o componente.

Applicazione dei criteri

I criteri sono applicati nell'ordine in cui sono organizzati i Gruppi statici. Al contrario, nei Gruppi dinamici vengono prima esplorati i Gruppi dinamici figli. In questo modo è possibile applicare criteri con un maggiore impatto nella parte superiore della struttura del Gruppo con criteri più specifici per i sottogruppi. Con criteri configurati adeguatamente con contrassegni, un utente ERA con accesso ai gruppi situati nel livello più alto della struttura possono ignorare i criteri dei Gruppi situati a un livello più basso. L'algoritmo è illustrato in maniera dettagliata nella sezione Modalità di applicazione dei criteri ai client.

Unione dei criteri

Un criterio applicato a un client è, di norma, il risultato di più criteri uniti in un criterio finale.

NOTA: è consigliabile assegnare più criteri generici (ad esempio impostazioni generali quali il server di aggiornamento) a gruppi situati a un livello più alto della struttura del gruppo. I criteri più specifici (ad esempio le impostazioni di controllo dei dispositivi) dovrebbero essere assegnati a un livello più profondo nella struttura del gruppo. Ciò perché in genere il criterio di livello inferiore sostituisce le impostazioni dei criteri di livello superiore durante l'unione (se non definito diversamente tramite i contrassegni dei criteri).

NOTA: se è applicato un criterio e l'utente decide di rimuoverlo in un secondo momento, alla rimozione del criterio la configurazione dei computer client non verrà ripristinata sulle impostazioni originali ma rimarrà invariata in base all'ultimo criterio applicato ai clienti. Ciò si verifica anche quando un computer diventa membro di un Gruppo dinamico al quale è applicato un determinato criterio che modifica le impostazioni del computer. Queste impostazioni rimangono invariate anche se il computer lascia il Gruppo dinamico. È pertanto consigliabile creare un criterio con impostazioni predefinite e assegnarlo al gruppo radice (**Tutti**) per ripristinare le impostazioni predefinite in una situazione del genere. In questo modo, quando un computer lascia un Gruppo dinamico che ne ha modificato le impostazioni, sul tale computer vengono ripristinate le impostazioni predefinite.

6.1.2.1 Procedura guidata criteri

È possibile utilizzare i criteri di configurazione del prodotto ESET come si farebbe dalla finestra Configurazione avanzata dell'interfaccia utente grafica (GUI) del prodotto. Diversamente dai criteri in Active Directory, i criteri ERA non possono trasportare alcuno script o serie di comandi.

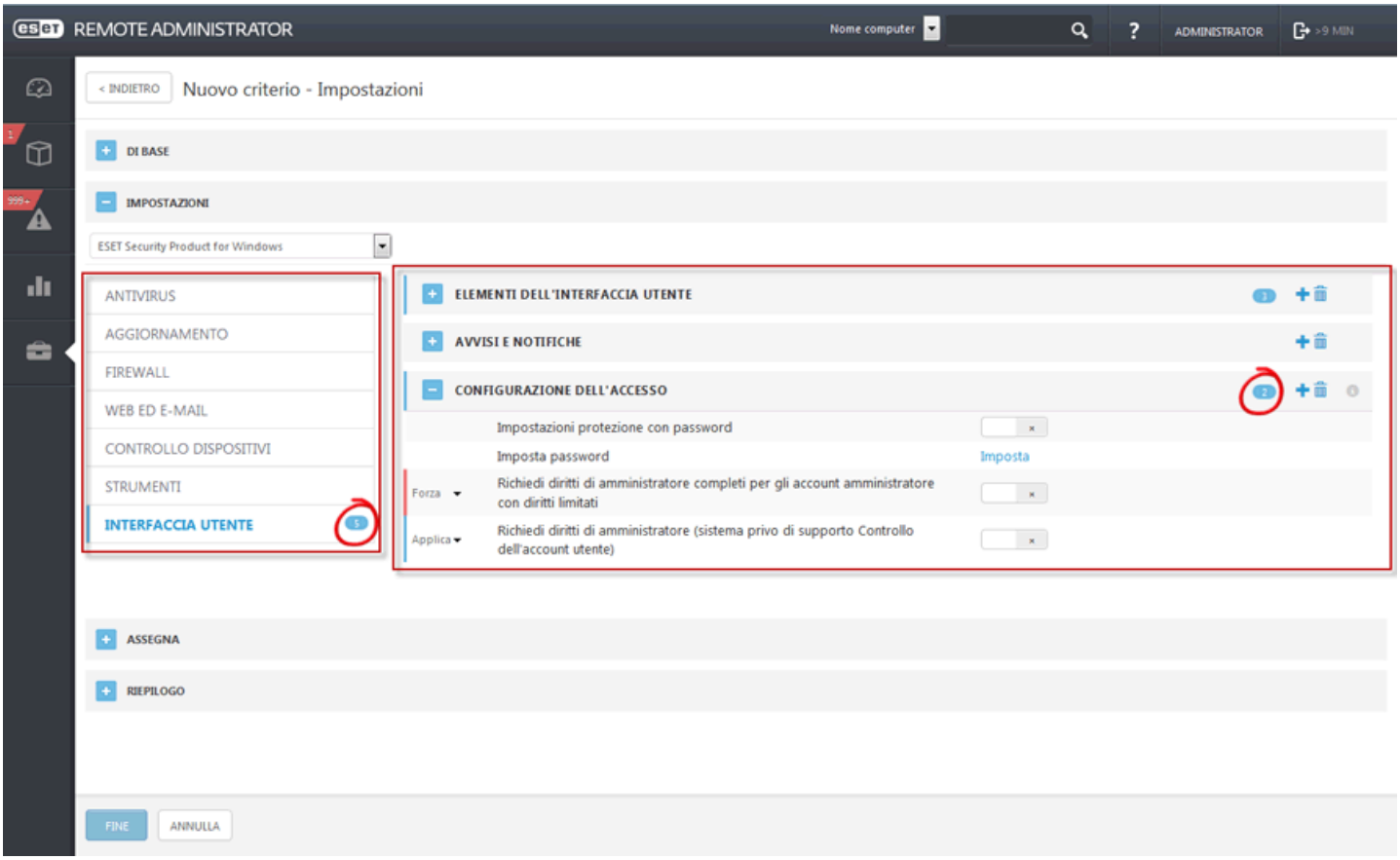
I criteri sono creati e gestiti nella scheda **Amministrazione** > **Criteri**. Fare clic su **Criteri** in basso e selezionare Nuovo dal menu contestuale.

Di base

Specificare un **Nome** per il nuovo criterio. Il campo **Descrizione** è facoltativo.

Impostazioni

Selezionare il prodotto dal menu a discesa.



Selezionare una categoria nella struttura ad albero sulla sinistra. Nel riquadro sulla destra, modificare le impostazioni, se necessario. Ciascuna impostazione rappresenta una regola per la quale è possibile definire un contrassegno. Per facilitare la navigazione, vengono contate tutte le regole. Il numero di regole definite dall'utente in una particolare sezione verrà visualizzato automaticamente. Sarà inoltre possibile visualizzare un numero accanto al nome di una categoria nella struttura ad albero sulla sinistra. Questa sezione consente di visualizzare una panoramica delle regole in tutte le relative sezioni. In tal modo, sarà possibile offrire all'utente una rapida panoramica del numero di impostazioni o regole definite e del punto in cui viene eseguita tale operazione.

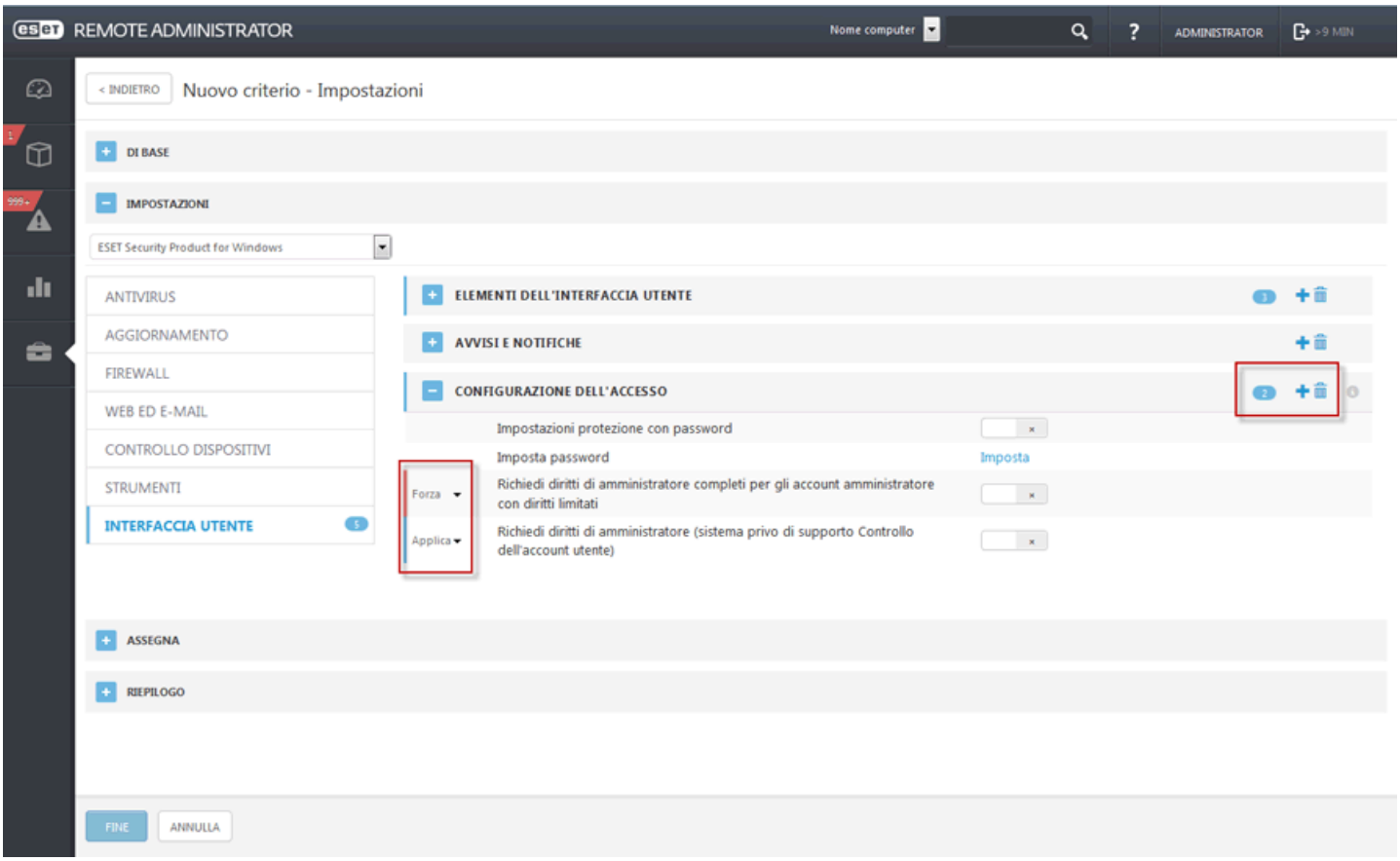
Per facilitare la modifica dei criteri, è anche possibile utilizzare i seguenti suggerimenti:

- utilizzare + per impostare il contrassegno **Applica** a tutte le voci in una sezione corrente
- eliminare le regole utilizzando l'icona del **Cestino**

6.1.2.2 Contrassegni

È possibile impostare un contrassegno per ciascuna impostazione in un criterio. I contrassegni definiscono le modalità di gestione di un'impostazione da parte del criterio:

- Applica: le impostazioni con questo contrassegno verranno inviate al client. Tuttavia, in caso di unione di criteri, può essere sovrascritto da un criterio successivo. Quando un criterio viene applicato a un computer client e una specifica impostazione presenta questo contrassegno, tale impostazione viene modificata indipendentemente da ciò che è stato configurato a livello locale sul client. Poiché l'impostazione non viene forzata, può essere modificata successivamente da altri criteri.
- Forza: le impostazioni con questo contrassegno hanno priorità e non possono essere sovrascritte da un criterio successivo, anche qualora esso stesso sia associato a tale contrassegno. In questo modo si assicura che l'impostazione non verrà modificata da criteri successivi in fase di unione.



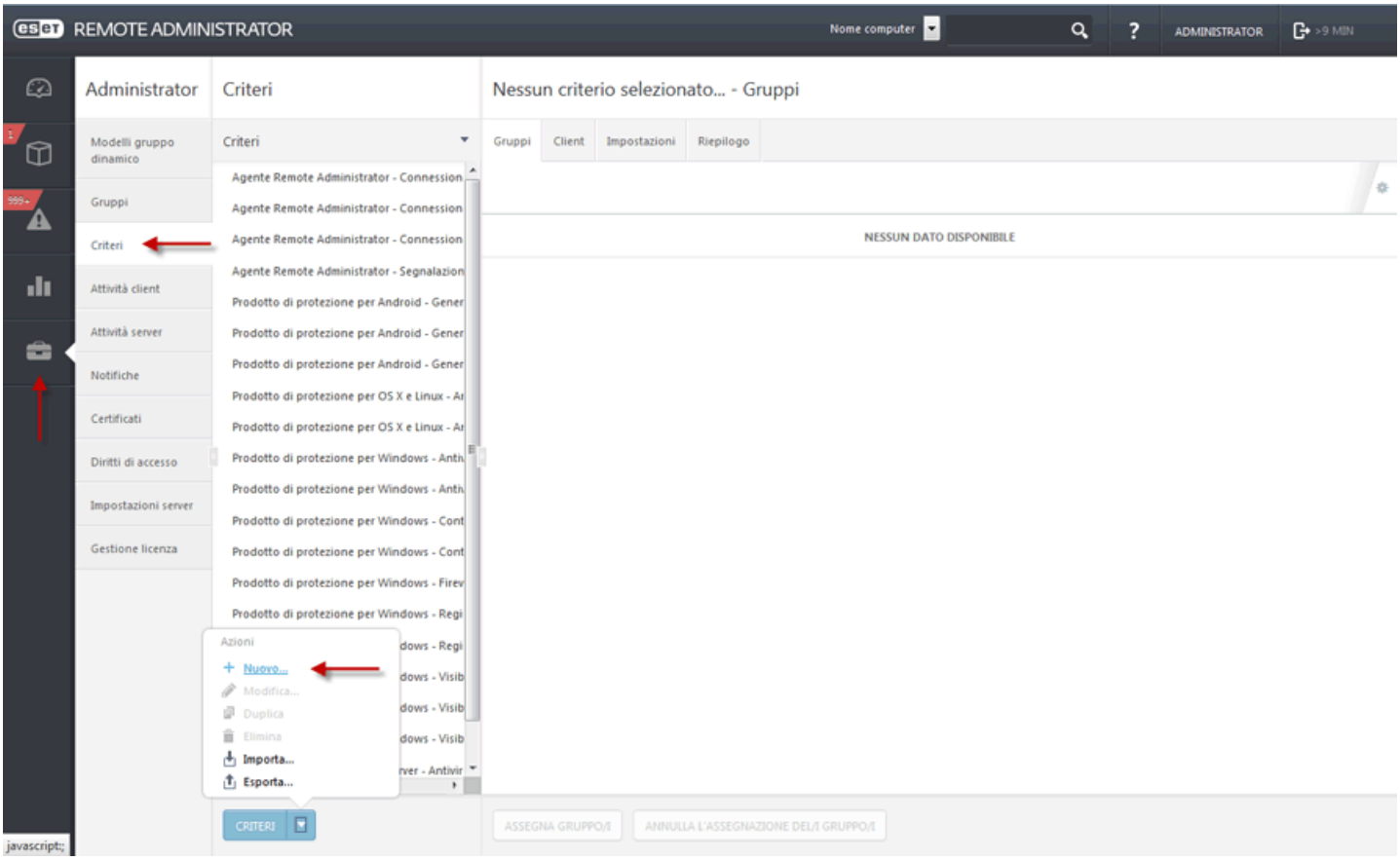
Selezionare una categoria nella struttura ad albero sulla sinistra. Nel riquadro sulla destra, modificare le impostazioni, se necessario. Ciascuna impostazione rappresenta una regola per la quale è possibile definire un contrassegno. Per facilitare la navigazione, vengono contate tutte le regole. Il numero di regole definite dall'utente in una particolare sezione verrà visualizzato automaticamente. Sarà inoltre possibile visualizzare un numero accanto al nome di una categoria nella struttura ad albero sulla sinistra. Questa sezione consente di visualizzare una panoramica delle regole in tutte le relative sezioni. In tal modo, sarà possibile offrire all'utente una rapida panoramica del numero di impostazioni o regole definite e del punto in cui viene eseguita tale operazione.

Per facilitare la modifica dei criteri, è anche possibile utilizzare i seguenti suggerimenti:
- utilizzare + per impostare il contrassegno **Applica** a tutte le voci in una sezione corrente
- eliminare le regole utilizzando l'icona del **Cestino**

6.1.2.3 Gestisci criteri

Nell'esempio verrà creato un nuovo criterio per l'intervallo di connessione dell'agente ERA. Si consiglia vivamente di eseguire questa operazione prima di effettuare i test sulla distribuzione di massa nell'ambiente d'uso.

1. Creare un nuovo gruppo statico.
2. Aggiungere un nuovo criterio facendo clic su **Amministrazione** > **Criteri**. Fare clic su **Criteri** nella parte inferiore e selezionare **Nuovo**.

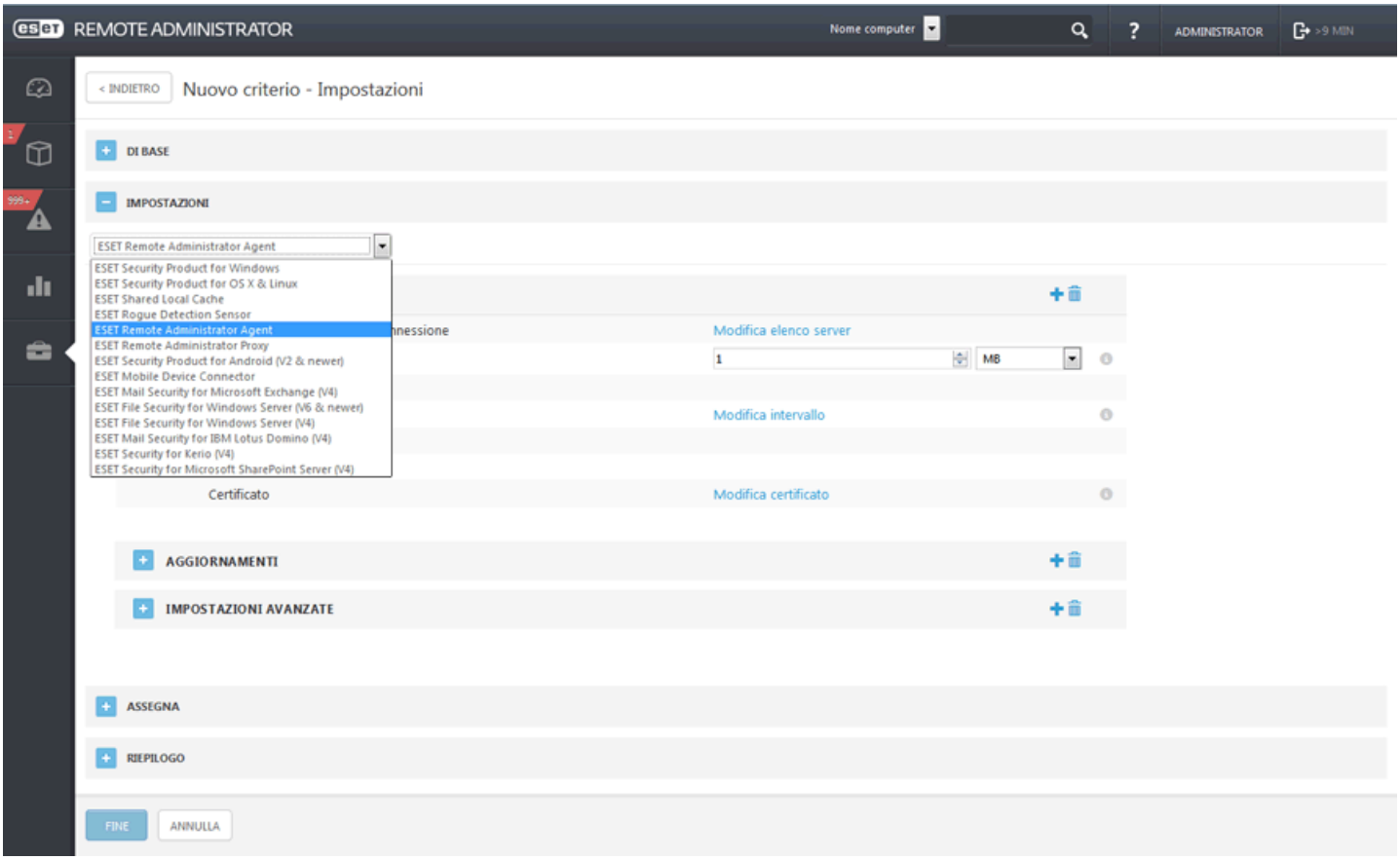


Di base

Immettere un **Nome** per il nuovo criterio (ad esempio, "Intervallo di connessione agente"). Il campo **Descrizione** è facoltativo.

Impostazioni

Selezionare **Agente ESET Remote Administrator** dal menu a discesa **Prodotto**.



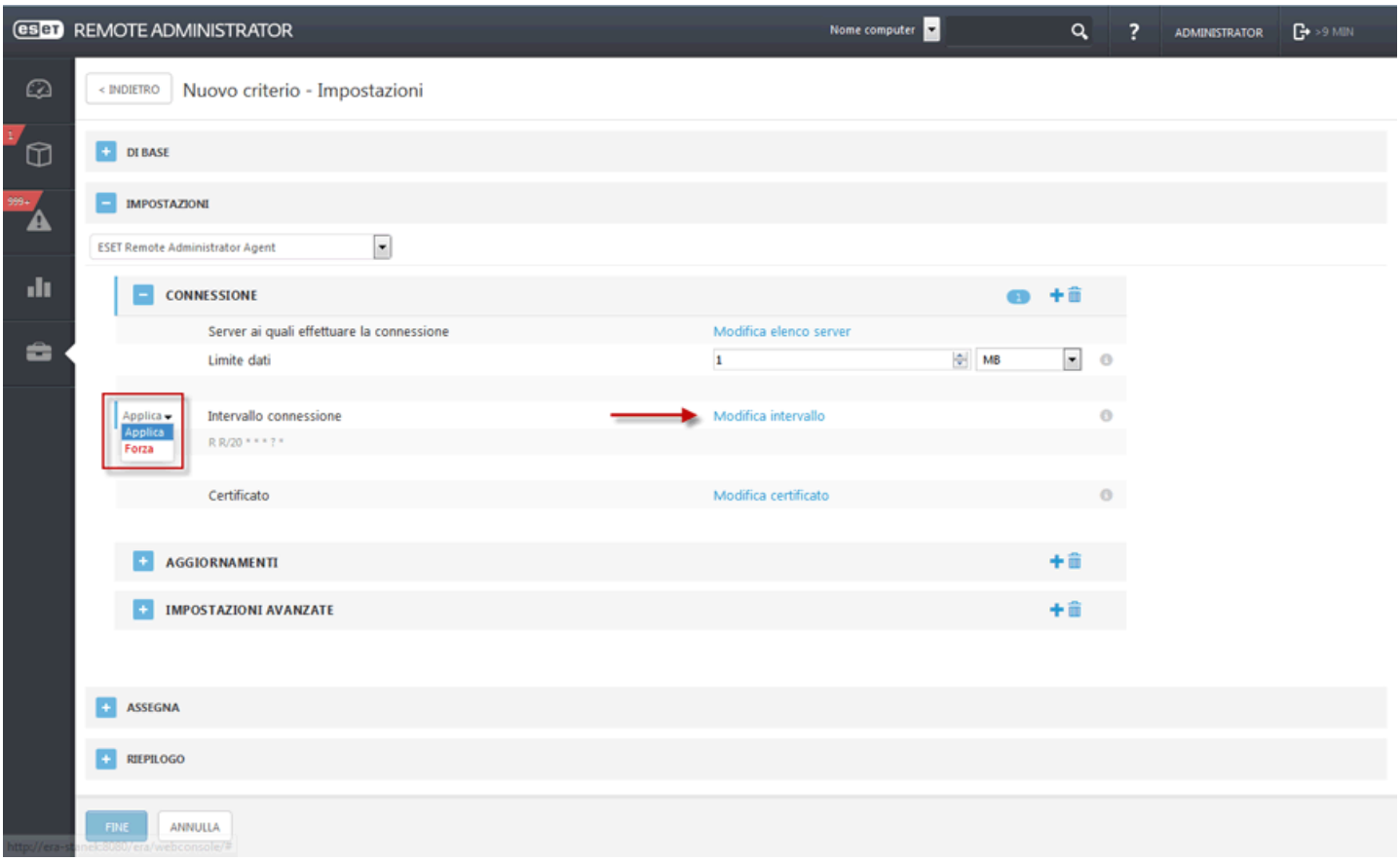
Connessione

Selezionare una categoria nella struttura ad albero sulla sinistra. Nel riquadro sulla destra, modificare le impostazioni, se necessario. Ciascuna impostazione rappresenta una regola per la quale è possibile definire un contrassegno. Per facilitare la navigazione, vengono contate tutte le regole. Il numero di regole definite dall'utente in una particolare sezione verrà visualizzato automaticamente. Sarà inoltre possibile visualizzare un numero accanto al nome di una categoria nella struttura ad albero sulla sinistra. Questa sezione consente di visualizzare una panoramica delle regole in tutte le relative sezioni. In tal modo, sarà possibile offrire all'utente una rapida panoramica del numero di impostazioni o regole definite e del punto in cui viene eseguita tale operazione.

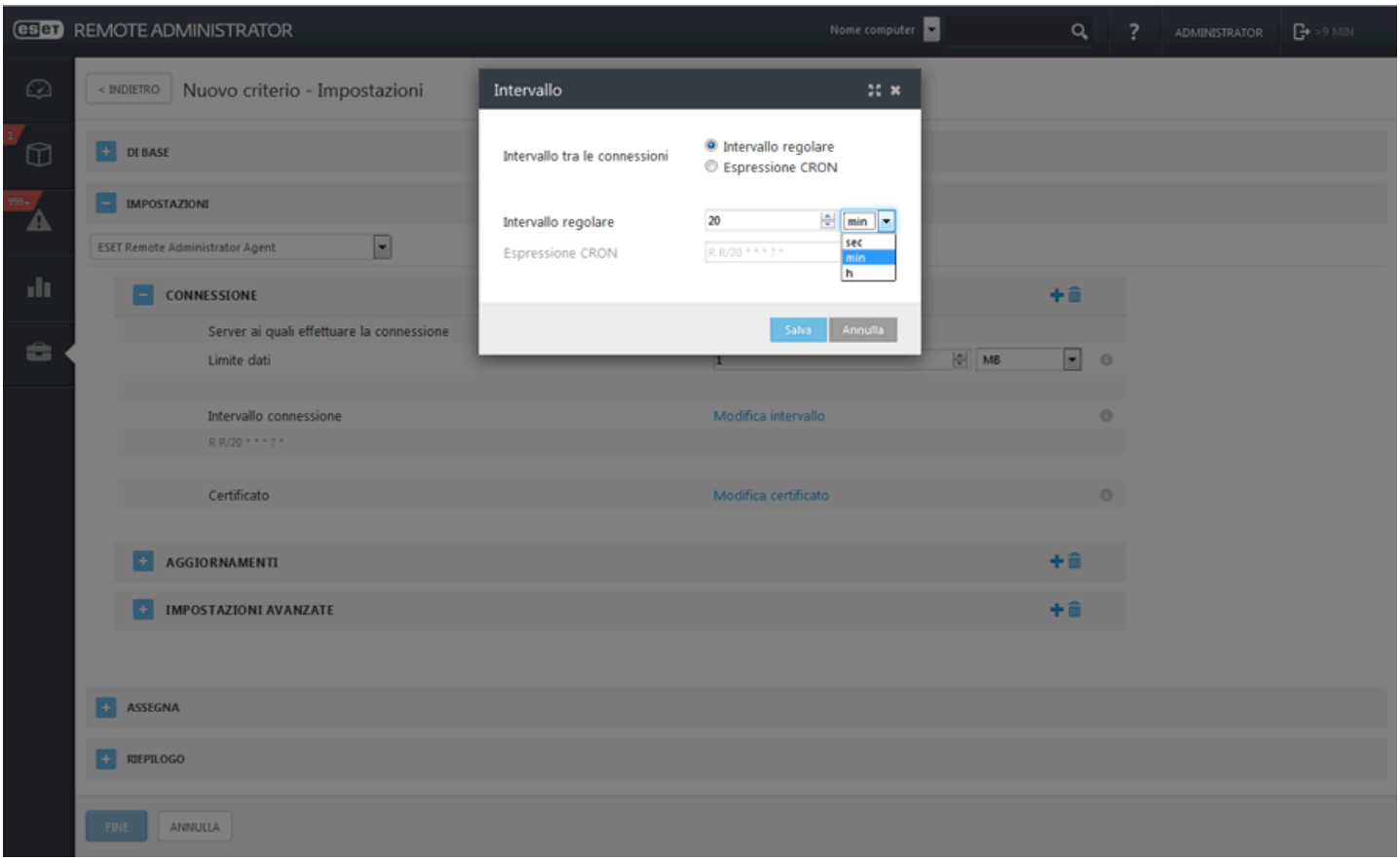
Per facilitare la modifica dei criteri, è anche possibile utilizzare i seguenti suggerimenti:

- utilizzare + per impostare il contrassegno **Applica** a tutte le voci in una sezione corrente
- eliminare le regole utilizzando l'icona del **Cestino**

Fare clic su **Modifica intervallo**.



Nel campo **Intervallo regolare**, impostare il valore dell'intervallo desiderato (si consiglia 60 secondi) e fare clic su Salva.



Dopo aver creato un nuovo criterio per l'intervallo di connessione dell'agente, assegnarlo al gruppo statico creato nel passaggio 1.

Dopo aver terminato i test sulla distribuzione di massa, modificare le impostazioni del criterio per l'intervallo di connessione dell'agente ERA create al passaggio 2.

Fare clic su **Amministrazione** > **Gruppi** e selezionare la scheda **Criteri**. Fare clic sul criterio per l'intervallo di connessione dell'agente, scegliere **Modifica**, quindi fare clic su **Impostazioni** > **Connessione**. Fare clic su **Modifica intervallo** e impostare l'intervallo di connessione su 20 minuti.

6.1.2.4 Modalità di applicazione dei criteri ai client

Ai Gruppi e ai Computer possono essere applicati diversi criteri. Un Computer può inoltre trovarsi in un Gruppo estremamente nidificato, i cui padri hanno i propri criteri.

L'aspetto più importante per l'applicazione dei criteri è il rispettivo ordine che viene derivato dall'ordine del Gruppo e dall'ordine dei criteri assegnati al Gruppo.

Attenersi ai passaggi seguenti per determinare il criterio attivo per qualsiasi client:

1. Trovare l'ordine dei gruppi in cui risiede il client
2. Sostituire i gruppi con criteri assegnati
3. Unire i criteri per ottenere le impostazioni finali

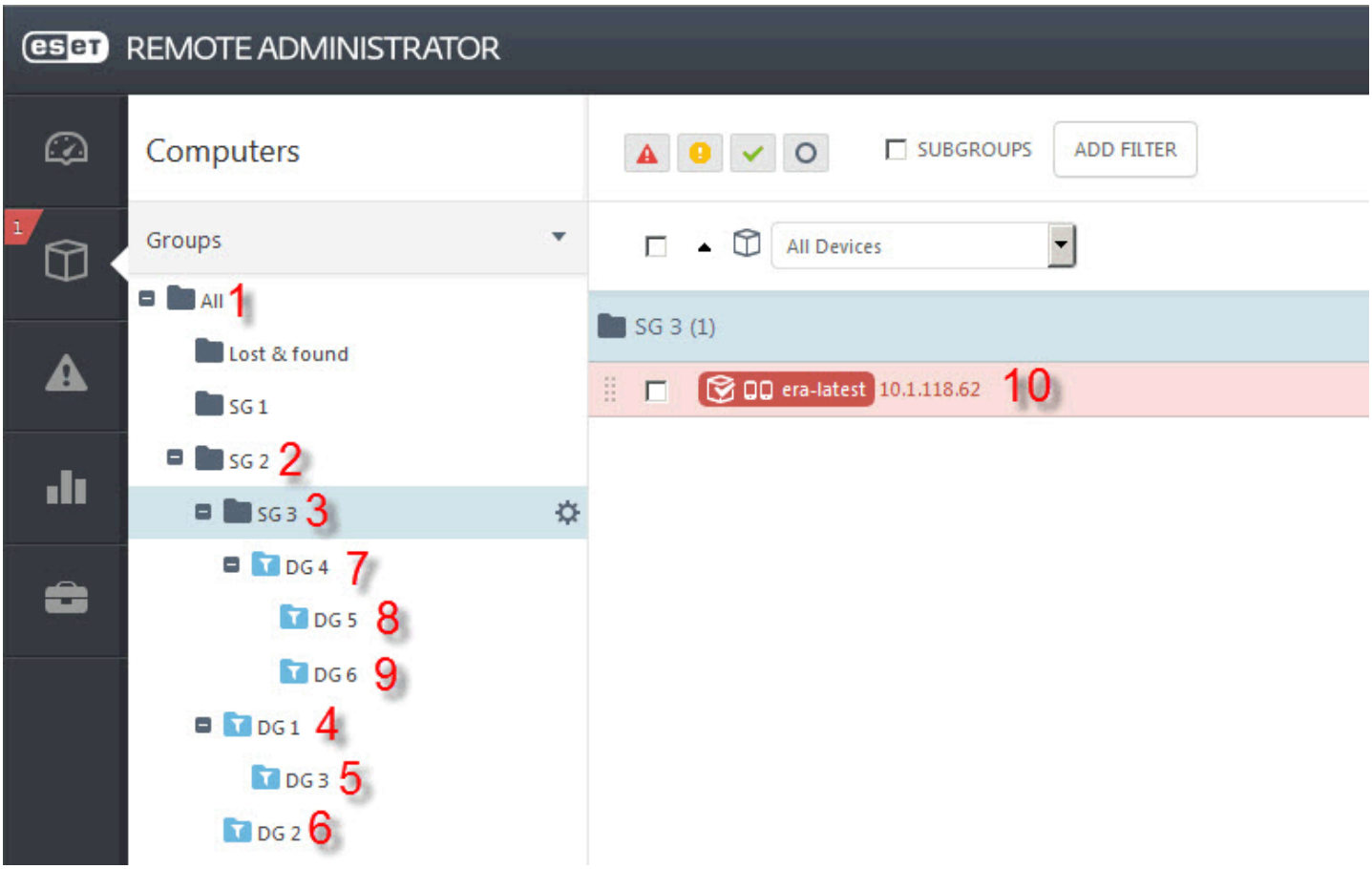
6.1.2.4.1 Ordinamento dei gruppi

Ai **Gruppi** possono essere assegnati **Criteri** che sono applicati in un ordine specifico.

Quando si ordinano i Gruppi nell'elenco vengono applicate diverse regole:

1. I Gruppi statici vengono esplorati dal Gruppo statico radice - Tutto.
2. Su ogni livello, i Gruppi statici di tale livello vengono esplorati per primi nell'ordine in cui appaiono nella struttura: questo metodo è anche noto come Ricerca in ampiezza.
3. Dopo che tutti i Gruppi statici a un determinato livello sono nell'elenco vengono esplorati i Gruppi dinamici.
4. In ogni Gruppo dinamico, tutti i relativi figli vengono esplorati nell'ordine in cui appaiono nell'elenco.
5. A qualsiasi livello dei Gruppi dinamici, se è presente un figlio, viene elencato e viene eseguita la ricerca dei relativi figli. Quando non sono più presenti figli, vengono elencati i successivi Gruppi dinamici a livello padre: questo metodo è anche noto come Ricerca in profondità.
6. L'esplorazione termina su un Computer.

In pratica, l'esplorazione è simile alla seguente:



Come mostrato sopra, la radice (Gruppo statico noto come Tutto) è elencata come **Regola 1**. Poiché non sono presenti altri gruppi allo stesso livello del gruppo Tutto, vengono valutati i criteri dei gruppi al livello successivo.

Vengono valutati successivamente i Gruppi statici Smarrito e ritrovato, SG 1 e SG 2. Il computer è in realtà solo un membro dei Gruppi statici Tutto/SG 2/SG 3 e, pertanto, non è necessario esplorare i gruppi Smarrito e ritrovato e SG 1. SG 2 è l'unico gruppo a questo livello che sarà valutato e, quindi, viene inserito nell'elenco e l'esplorazione viene eseguita a livelli più profondi.

Al terzo livello, l'algoritmo trova SG 3, DG 1 e DG 2. In base alla **Regola 2**, vengono prima elencati i Gruppi statici. L'esplorazione aggiunge SG 3 e poiché è l'ultimo Gruppo statico a livello 3, si sposta su DG 1. Prima di passare a DG 2 al livello 3, è necessario che siano elencati i figli di DG 1.

DG 3 viene aggiunto. Non avendo figli, l'esplorazione sale di livello.

DG 2 viene elencato. Non ha figli. A livello 3, non sono presenti altri gruppi. L'esplorazione passa al livello 4.

A livello 4 è presente solo il Gruppo dinamico DG 4 e il computer. La **Regola 6** stabilisce che il computer deve essere posizionato per ultimo, quindi viene scelto DG 4. DG 4 ha due figli che devono essere elaborati prima di poter procedere.

DG 5 e DG6 vengono aggiunti all'elenco. Entrambi non hanno figli e l'esplorazione non ha altri elementi da elaborare. Aggiunge Computer e viene completata.

L'elenco finale è quindi il seguente:

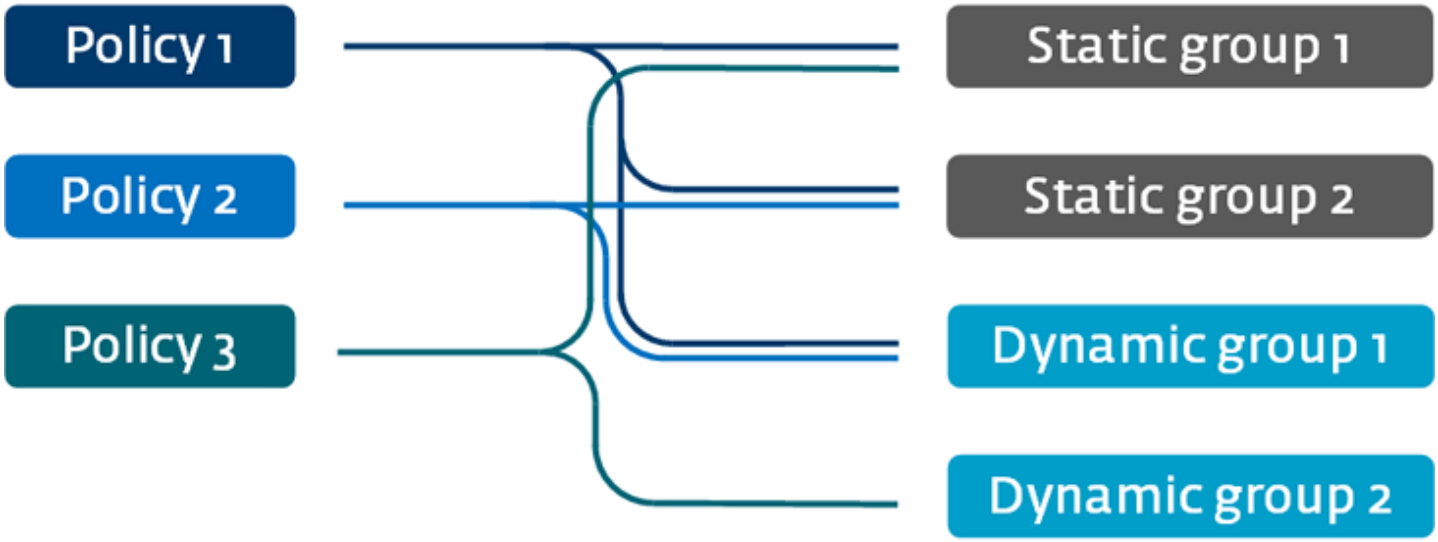
1. Tutto
2. SG 2
3. SG 3
4. DG 1
5. DG 3
6. DG 2
7. DG 4
8. DG 5
9. DG 6
10. Computer

Questo è l'ordine in cui i Criteri vengono applicati.

6.1.2.4.2 Enumerazione dei criteri

Quando è noto l'ordine dei gruppi, si può procedere alla sostituzione di ciascun gruppo con i criteri assegnati a esso. I criteri sono elencati nello stesso ordine in cui sono assegnati a un Gruppo. Un gruppo senza un criterio viene rimosso dall'elenco. È possibile modificare la priorità dei criteri per un gruppo con più criteri assegnati. Ciascun criterio configura esclusivamente un prodotto (agente ERA, proxy ERA, EES, ecc.)

Si prendano in esame 3 criteri applicati ai Gruppi statici e dinamici (vedere immagine seguente):



L'elenco dal punto 1 sarebbe trasformato come segue:

1. Tutti (rimossi, nessun Criterio)
2. SG 2 -> Criterio 1, Criterio 2
3. SG 3 (rimosso per assenza di Criterio)
4. DG 1 -> Criterio 1, Criterio 2
5. DG 3 (rimosso per assenza di Criterio)
6. DG 2 -> Criterio 3
7. DG 4 (rimosso per assenza di Criterio)
8. DG 5 (rimosso per assenza di Criterio)
9. DG 6 (rimosso per assenza di Criterio)
10. Computer (rimosso per assenza di Criterio)

L'elenco finale dei Criteri è il seguente:

1. Criterio 1
2. Criterio 2
3. Criterio 1
4. Criterio 2
5. Criterio 3

6.1.2.4.3 Unione dei criteri

I criteri vengono uniti uno per uno. Durante l'unione dei criteri, la regola generale è che l'ultimo criterio sostituisce sempre le impostazioni definite dal precedente.
Per modificare tale comportamento è possibile utilizzare i contrassegni dei criteri (disponibili per ogni impostazione). Le impostazioni vengono unite una per una.

Tenere presente che la struttura dei gruppi (la loro gerarchia) e la sequenza dei criteri determina le modalità di unione dei criteri. L'unione di due qualsiasi criteri può produrre risultati differenti a seconda del relativo ordine. I gruppi sono stati ordinati e i criteri sono stati enumerati.

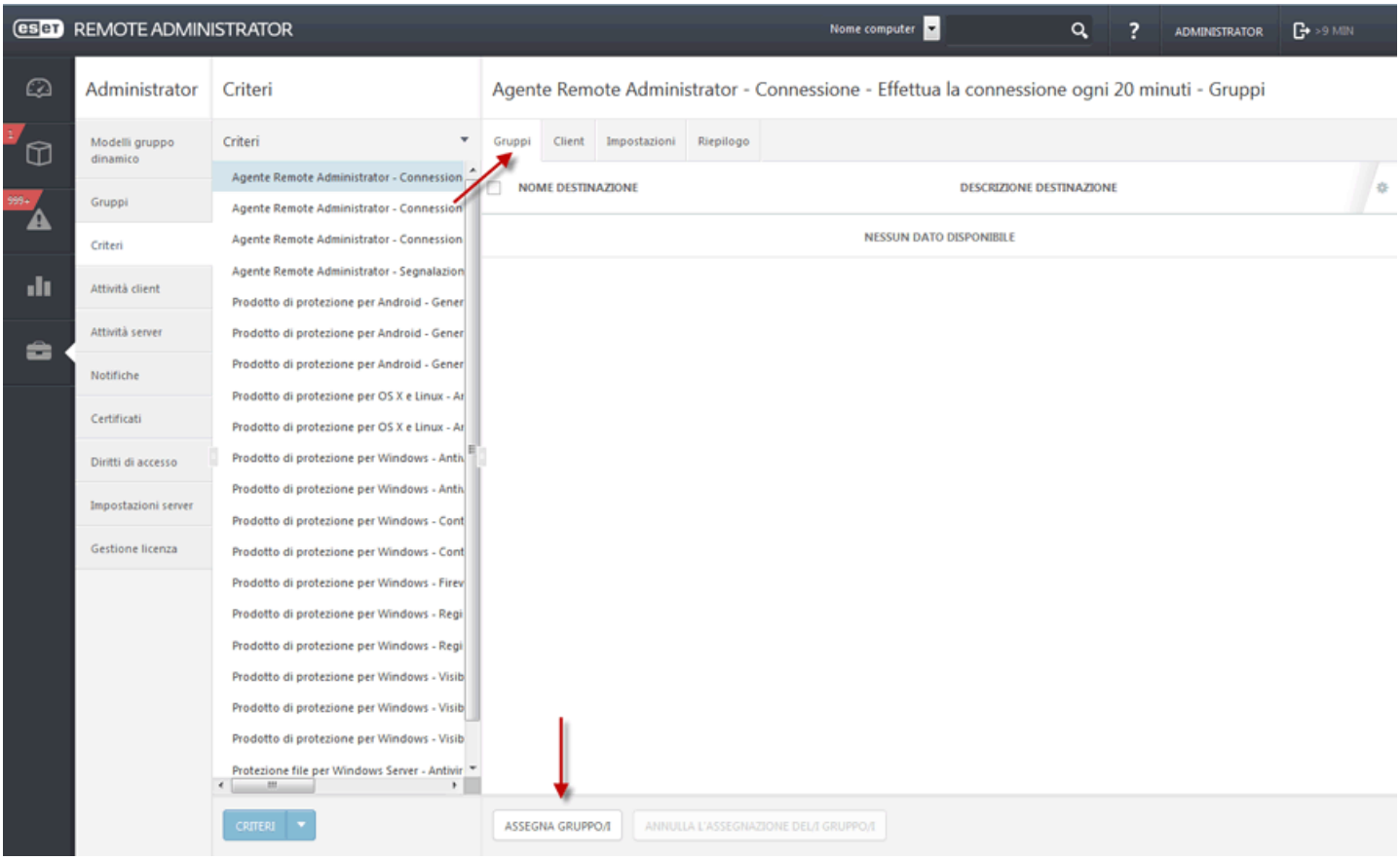
6.1.2.5 Configurazione di un prodotto da ERA

È possibile utilizzare i criteri di configurazione del prodotto ESET come si farebbe dalla finestra Configurazione avanzata dell'interfaccia utente grafica (GUI) del prodotto. Diversamente dai criteri in Active Directory, i criteri ERA non possono trasportare alcuno script o serie di comandi.

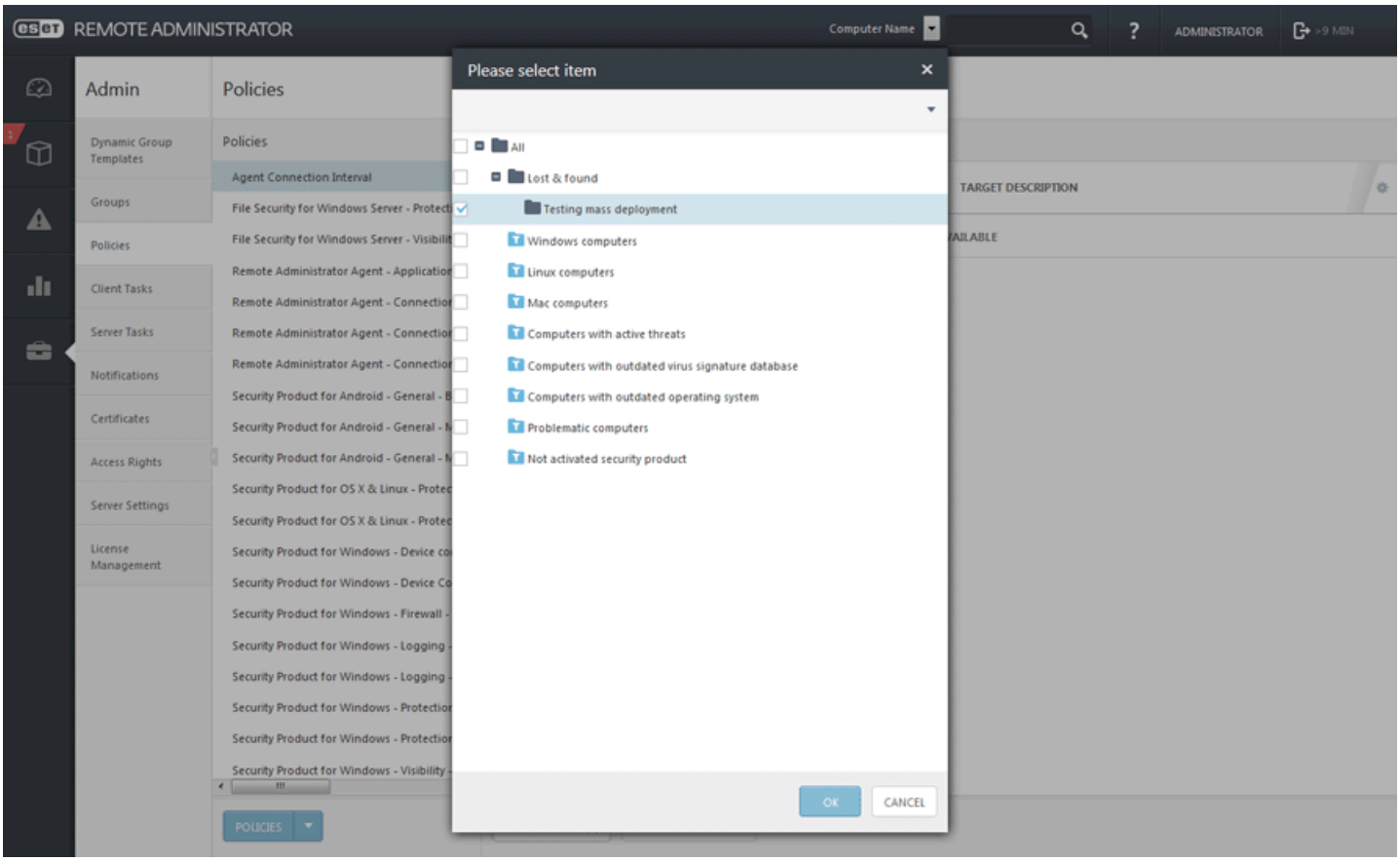
6.1.2.6 Assegna criterio a gruppo

Dopo aver creato un criterio, l'utente può assegnarlo a un **Gruppo statico** o **dinamico**. Un criterio può essere assegnato in due modi:

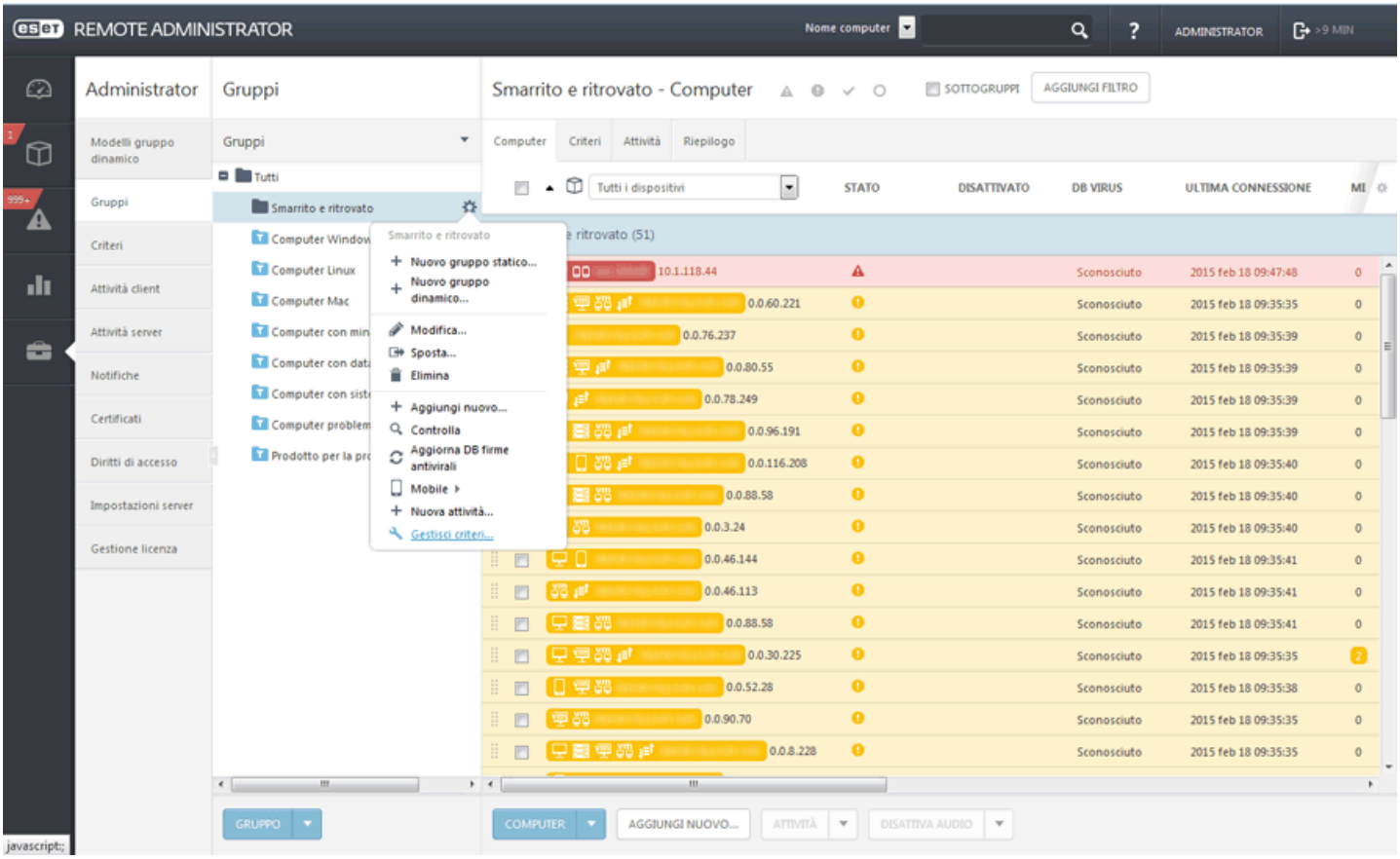
1. In **Amministrazione** > **Criteri** > selezionare un criterio e fare clic su **Assegna gruppo/i**. Selezionare un gruppo statico o dinamico e fare clic su **OK**.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Criteri
Agente Remote Administrator - Connessione - Effettua la connessione ogni 20 minuti - Gruppi
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
Criteri
Gruppi
Client
Impostazioni
Riepilogo
NOME DESTINAZIONE
DESCRIZIONE DESTINAZIONE
NESSUN DATO DISPONIBILE
Agente Remote Administrator - Connessione
Agente Remote Administrator - Connessione
Agente Remote Administrator - Connessione
Agente Remote Administrator - Segnalazioni
Prodotto di protezione per Android - Gener
Prodotto di protezione per Android - Gener
Prodotto di protezione per Android - Gener
Prodotto di protezione per OS X e Linux - Ar
Prodotto di protezione per OS X e Linux - Ar
Prodotto di protezione per Windows - Anth
Prodotto di protezione per Windows - Anti
Prodotto di protezione per Windows - Cont
Prodotto di protezione per Windows - Cont
Prodotto di protezione per Windows - Firev
Prodotto di protezione per Windows - Regi
Prodotto di protezione per Windows - Regi
Prodotto di protezione per Windows - Visib
Prodotto di protezione per Windows - Visib
Prodotto di protezione per Windows - Visib
Protezione file per Windows Server - Antivir
CRITERI
ASSEGNA GRUPPO/I
ANNULLA L'ASSEGNAZIONE DEL/I GRUPPO/I

Selezionare un **Gruppo** dall'elenco.



2. Fare clic su **Amministrazione** > **Gruppi** > **Gruppo** oppure sull'icona a forma di rotella accanto al nome del gruppo e selezionare **Gestisci criteri**.

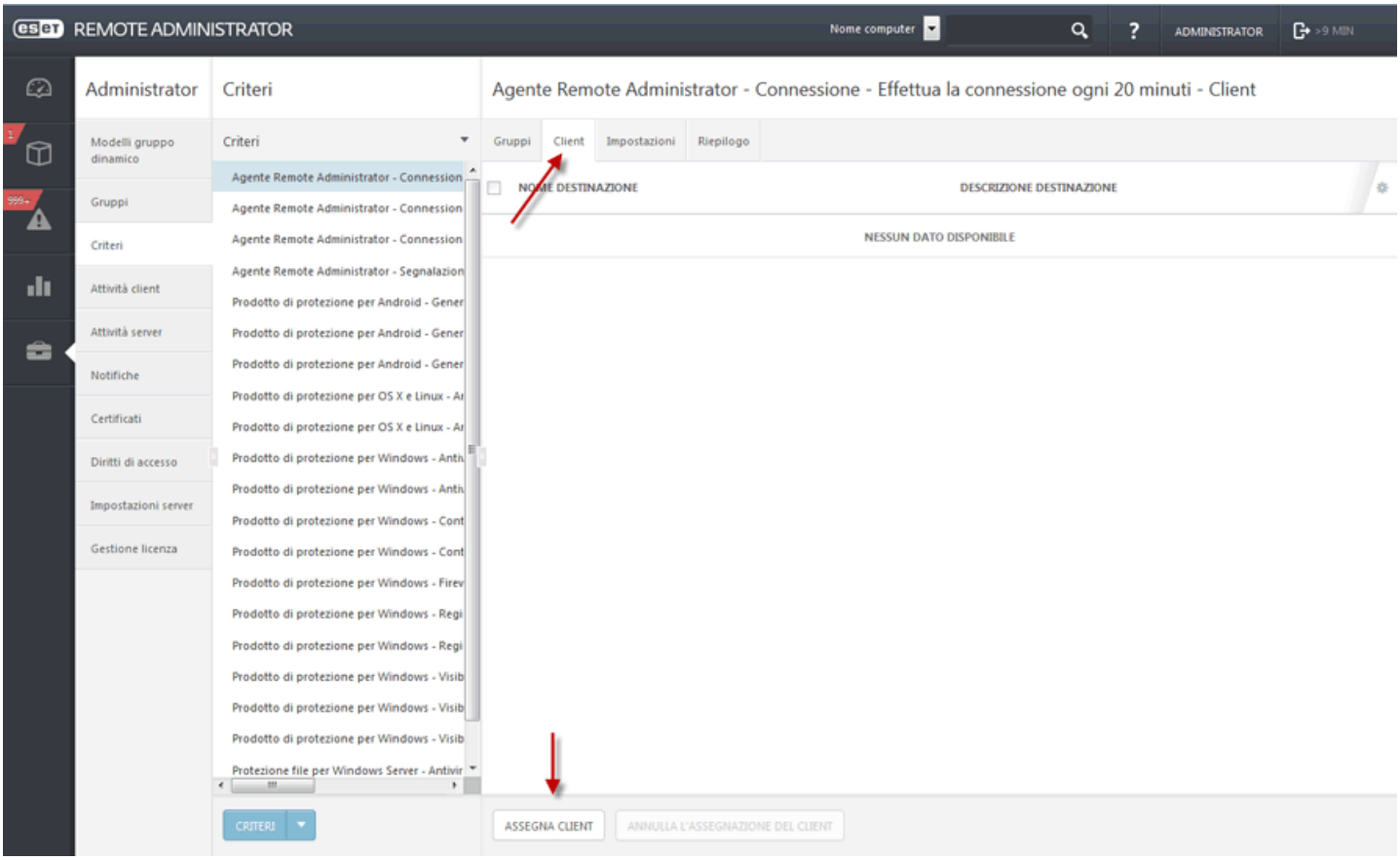


Nella finestra **Ordine applicazione criterio** fare clic su **Aggiungi criterio**. Selezionare la casella di controllo accanto al criterio che si desidera assegnare al gruppo e fare clic su **OK**.
Fare clic su **Salva**. Per visualizzare i criteri assegnati a un gruppo specifico, selezionarlo e fare clic sulla scheda **Criteri** per aprire un elenco di criteri assegnati al gruppo.

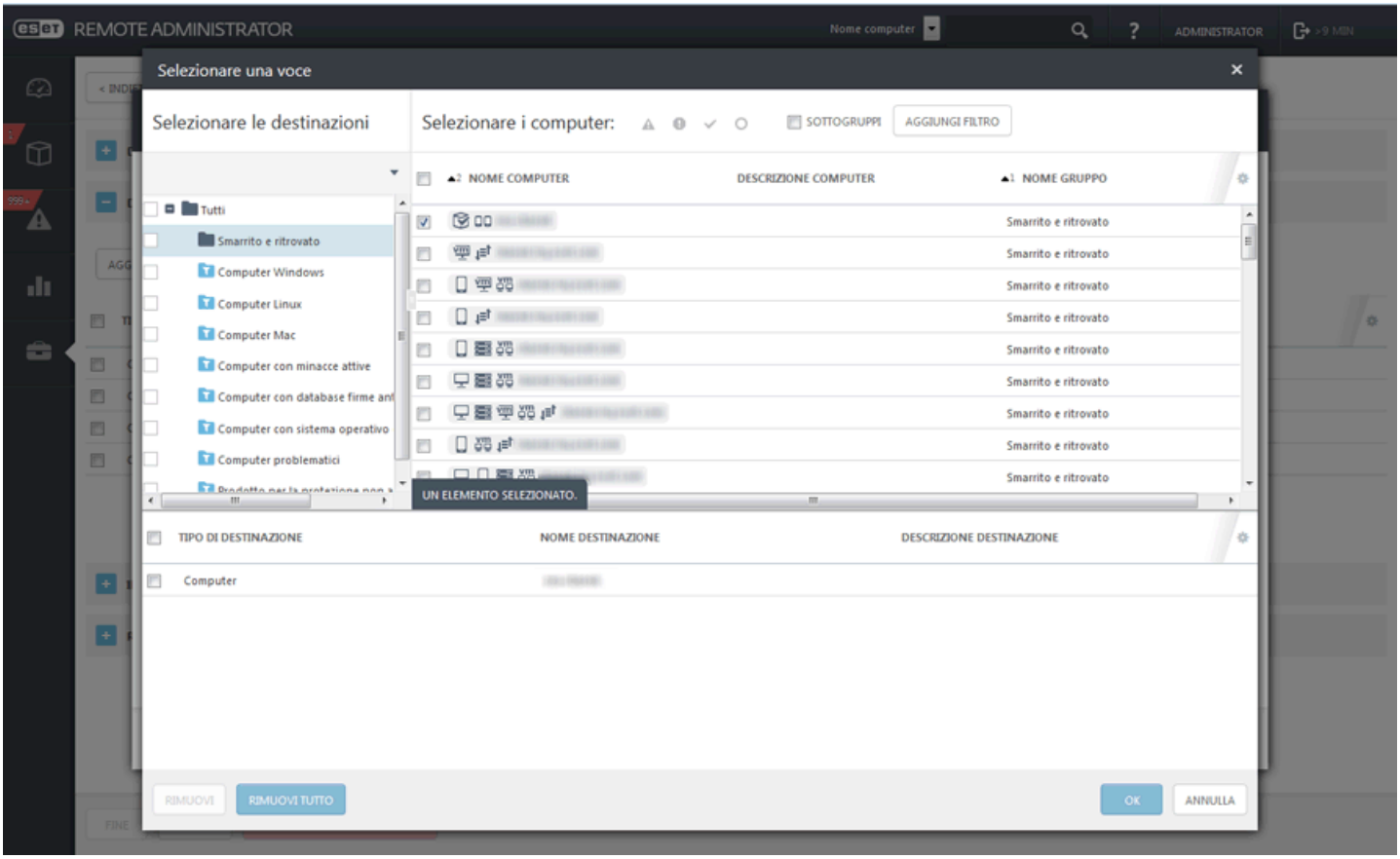
NOTA: per ulteriori informazioni sui criteri, consultare il capitolo Criteri.

6.1.2.7 Assegna un criterio a un client

Per assegnare un criterio a una workstation client, fare clic su **Amministrazione** > **Criteri** selezionare la scheda **Client** e fare clic su **Assegna client**.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Criteri
Agente Remote Administrator - Connessione - Effettua la connessione ogni 20 minuti - Client
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
Criteri
Agente Remote Administrator - Connession
Agente Remote Administrator - Connession
Agente Remote Administrator - Connession
Agente Remote Administrator - Segnalazion
Prodotto di protezione per Android - Gener
Prodotto di protezione per Android - Gener
Prodotto di protezione per Android - Gener
Prodotto di protezione per OS X e Linux - Ar
Prodotto di protezione per OS X e Linux - Ar
Prodotto di protezione per Windows - Anti
Prodotto di protezione per Windows - Anti
Prodotto di protezione per Windows - Cont
Prodotto di protezione per Windows - Cont
Prodotto di protezione per Windows - Firev
Prodotto di protezione per Windows - Regi
Prodotto di protezione per Windows - Regi
Prodotto di protezione per Windows - Visib
Prodotto di protezione per Windows - Visib
Prodotto di protezione per Windows - Visib
Protezione file per Windows Server - Antivir
CRITERI
Gruppi
Client
Impostazioni
Riepilogo
NOME DESTINAZIONE
DESCRIZIONE DESTINAZIONE
NESSUN DATO DISPONIBILE
ASSEGNA CLIENT
ANNULLA L'ASSEGNAZIONE DEL CLIENT

Selezionare i computer client di destinazione, quindi fare clic su **OK**. Il criterio sarà assegnato a tutti i computer selezionati.



6.1.3 Attività client

Per richiedere un'azione da un computer client è possibile utilizzare le **Attività client**. Le Attività client possono essere assegnate a gruppi o singoli computer. Una volta creata, l'attività viene eseguita in base al piano di programmazione. Dal momento che i client non sono sempre connessi al server ERA, la propagazione delle attività su di essi potrebbe richiedere del tempo. Per lo stesso motivo, potrebbe essere necessario del tempo prima che i risultati dell'esecuzione dell'attività siano restituiti al server ERA. Sono disponibili le seguenti attività predefinite:

Ciascuna **Categoria di attività** contiene **Tipi di attività:**

All Attività

- **Prodotto ESET Security**
  - Esporta configurazione prodotti gestiti
  - Controllo su richiesta
  - Attivazione prodotto
  - Gestione quarantena
  - Esegui script SysInspector
  - Richiesta rapporto SysInspector
  - Carica file in quarantena
  - Aggiornamento database firme antivirali
  - Rollback aggiornamento database firme antivirali
- **ESET Remote Administrator**
  - Aggiornamento componenti amministratore remoto

Reimposta agente clonato

Reimposta database Rogue Detection Sensor

Interrompi gestione (disinstallare agente ERA)

Sistema operativo

Visualizza messaggio

Aggiornamento sistema operativo

Esegui comando

Installazione software

Disinstallazione software

Interrompi gestione (disinstallare agente ERA)

Mobile

Azione Anti-Furto

Registrazione dispositivo

Visualizza messaggio

Esporta configurazione prodotti gestiti

Controllo su richiesta

Attivazione prodotto

Installazione software

Aggiornamento database firme antivirali

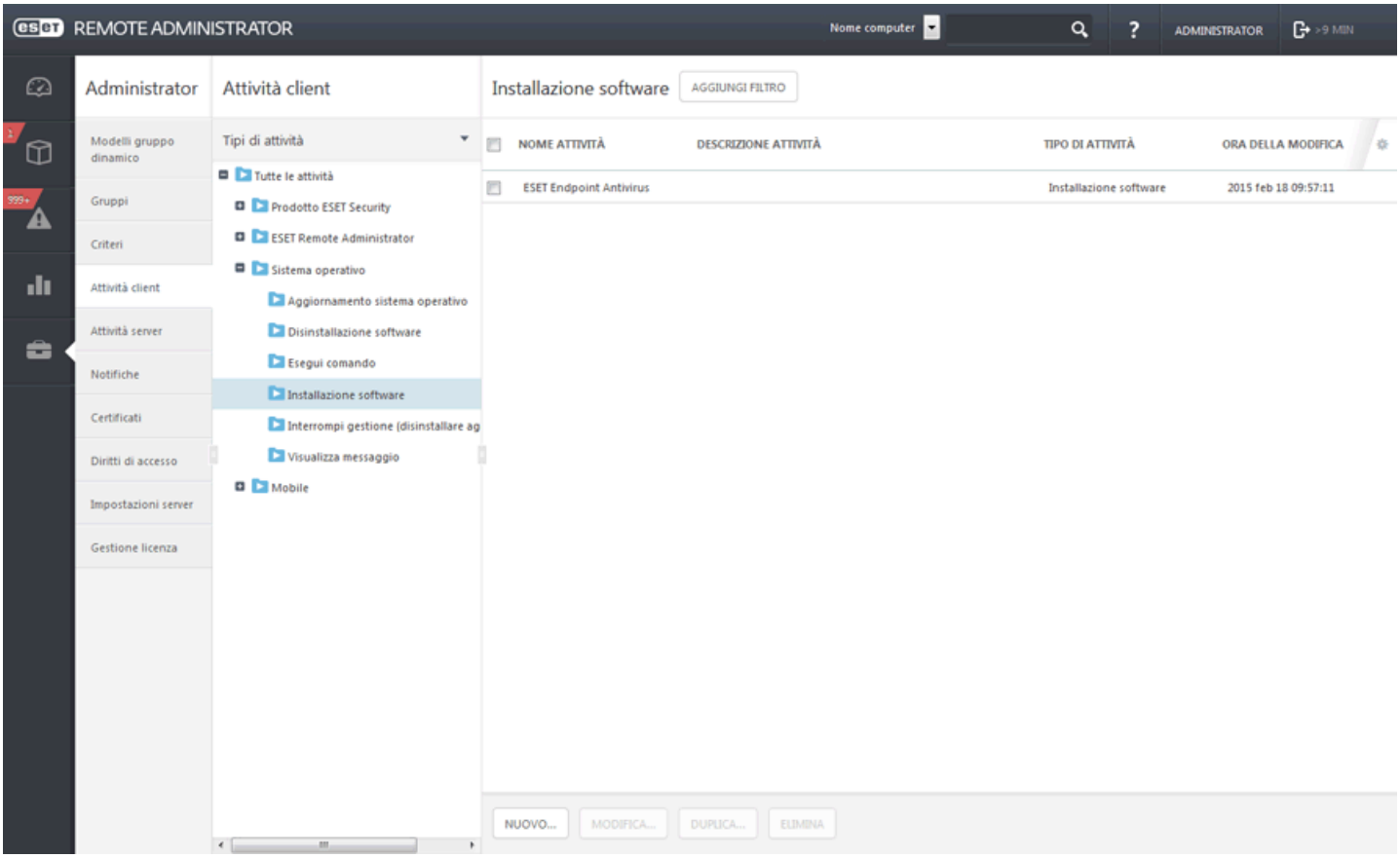
Interrompi gestione (disinstallare agente ERA)

6.1.3.1 Procedura guidata attività client

Le attività client sono create e gestite nella scheda **Amministrazione**. Fare clic su **Attività client**, selezionare un'attività dall'elenco **Tipi di attività**, quindi fare clic su **Nuovo.**

I prodotti di protezione ESET possono essere installati da remoto facendo clic sulla macchina desiderata e scegliendo **Nuovo**, o creando una nuova attività di **Installazione software** nel menu **Amministrazione** > **Attività client**. Fare clic su **Nuova...** per avviare la configurazione della nuova attività.

- Utilizzare le istruzioni che seguono oppure guardare il video illustrativo della Knowledge Base.

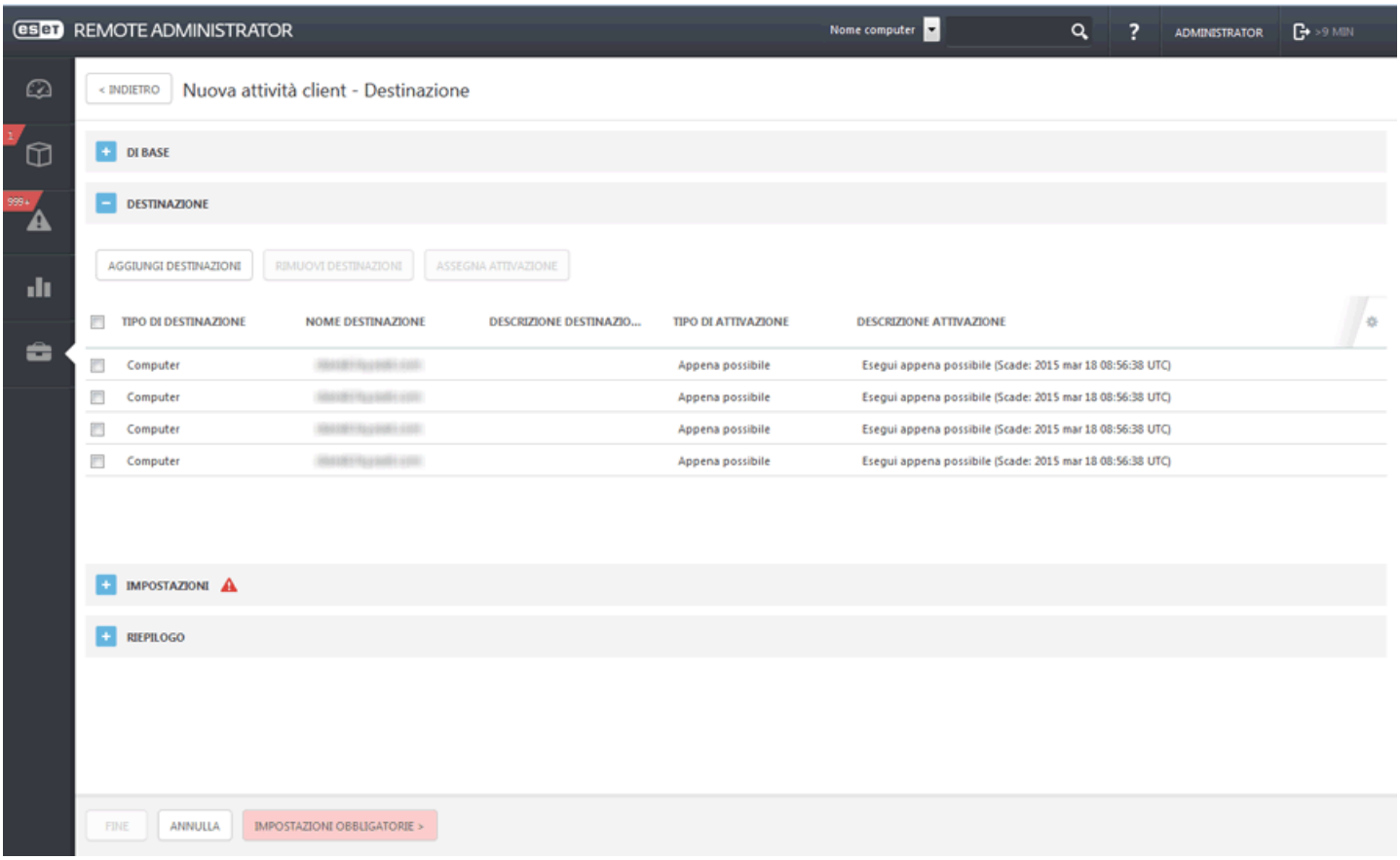


Di base

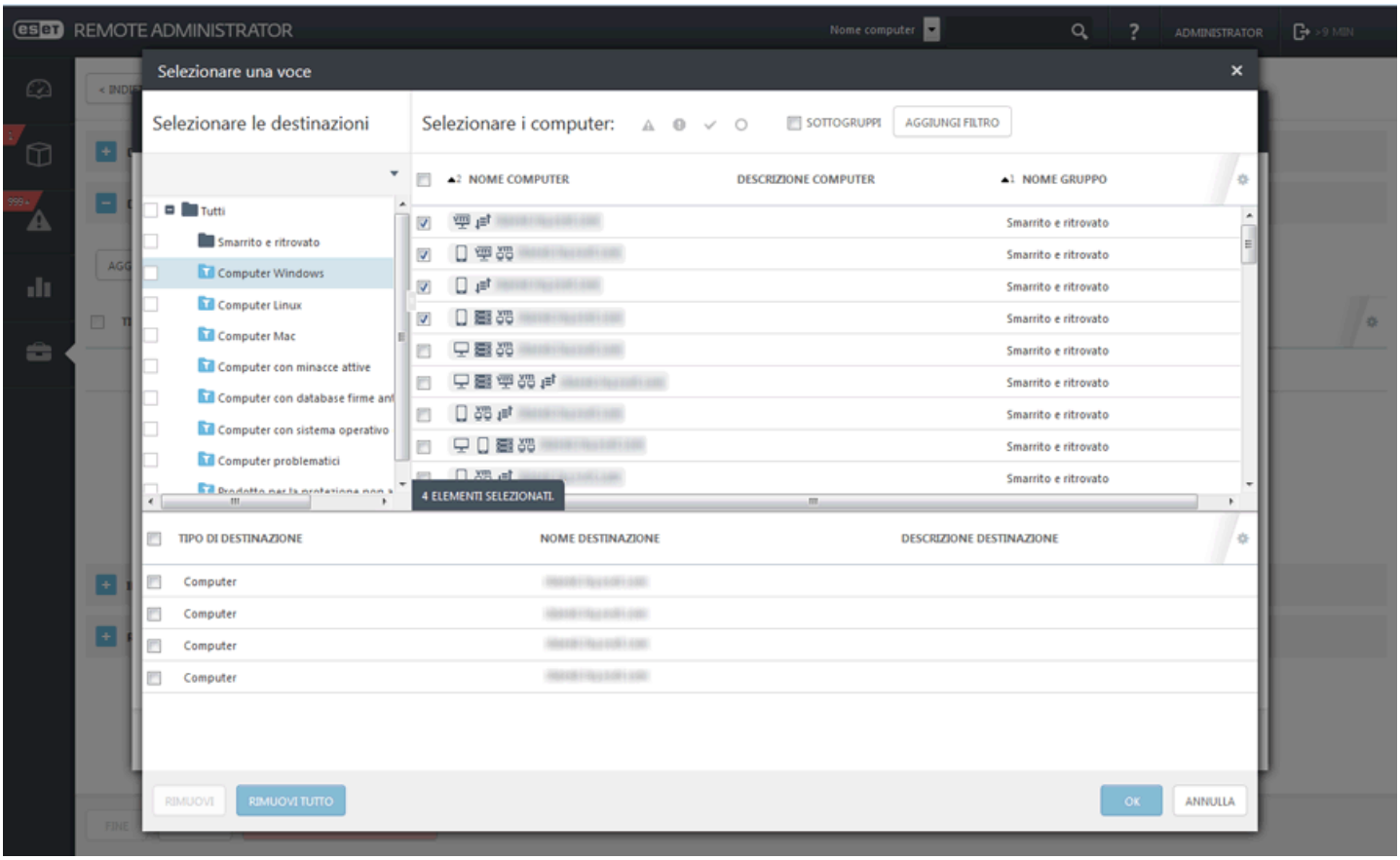
Inserire le informazioni di base sull'attività, come il **Nome**, la **Descrizione** facoltativa e il **Tipo di attività**. Il **Tipo di attività** (vedere l'elenco indicato in precedenza) definisce le impostazioni e il comportamento dell'attività. Selezionare l'attività **Installazione software**, quindi fare clic su **Destinazione**.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.

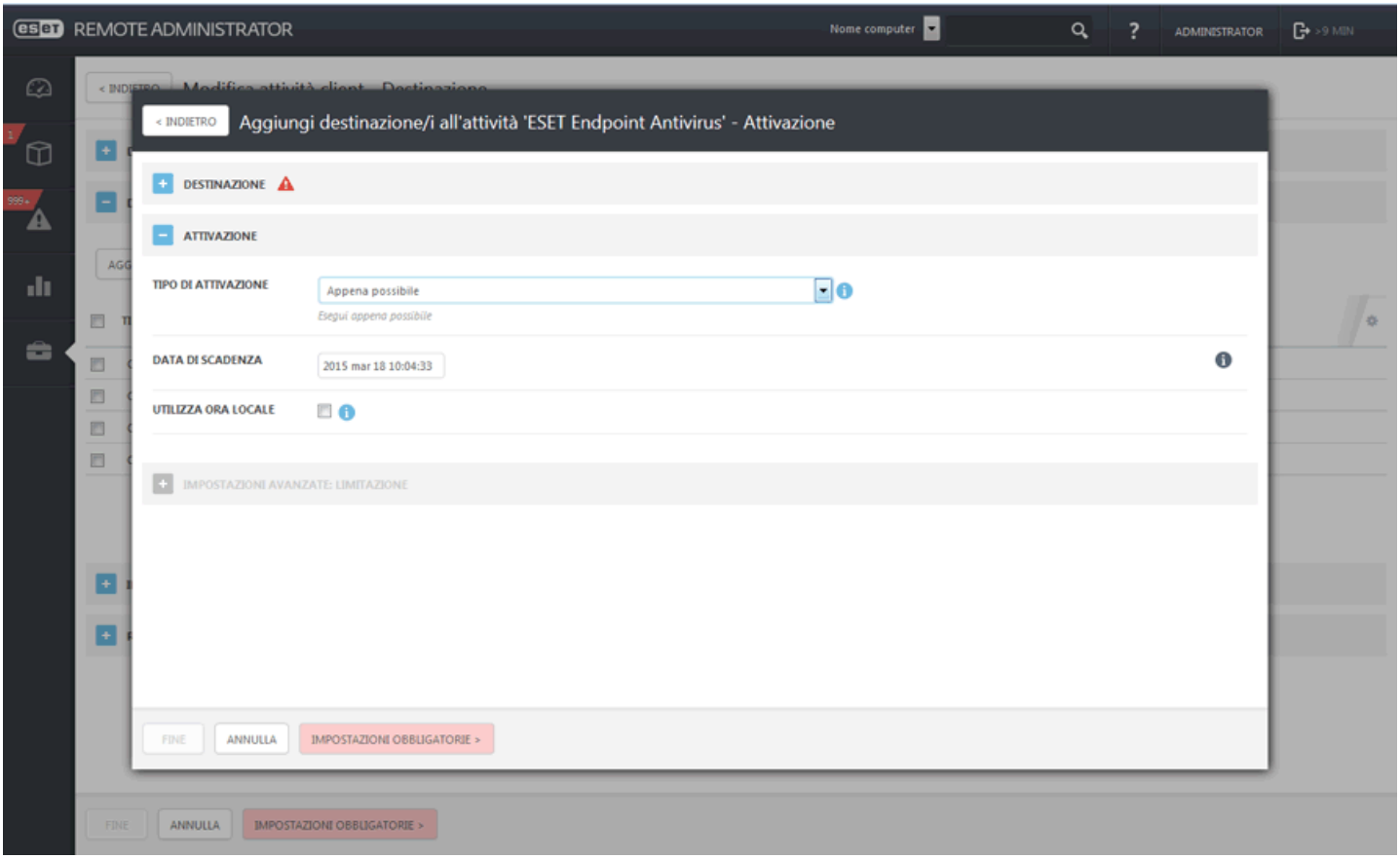


Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Attivazione

Come **Attivazione**, selezionare Esegui appena possibile. Tale operazione consentirà di inviare immediatamente l'attività ai client. L'opzione **Utilizza ora locale** fa riferimento all'ora locale del/i client e non del server.



Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per il momento, lasciare invariata l'opzione Limitazione delle richieste e fare clic su Fine per creare la nuova attività.

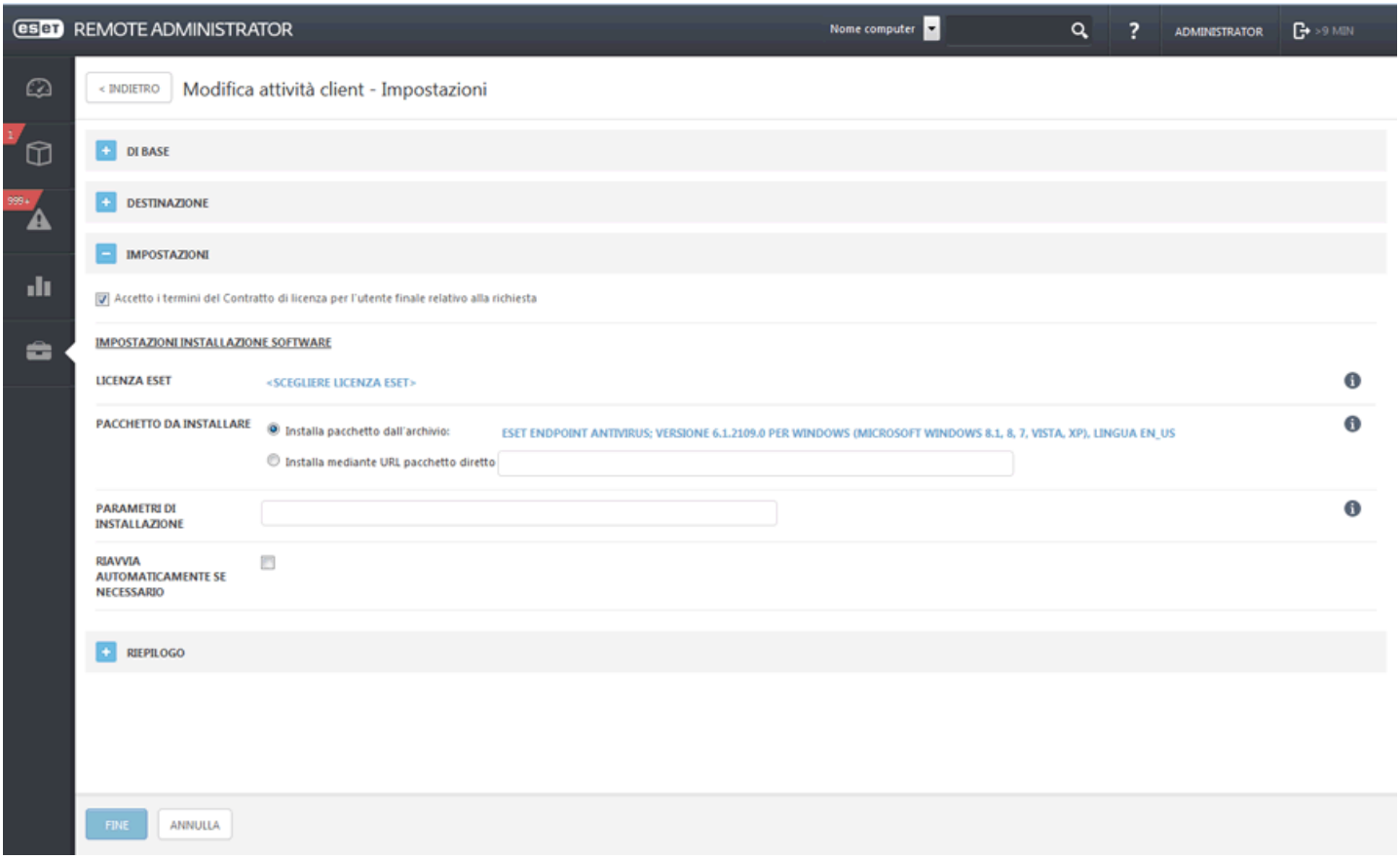
Impostazioni

Fare clic su **<Scegliere licenza ESET>** e selezionare la licenza appropriata per il prodotto installato nell'elenco di licenze disponibili. Se d'accordo, selezionare la casella di controllo accanto a **Accetto i termini del Contratto di licenza per l'utente finale relativo alla richiesta**. Per ulteriori informazioni, consultare il capitolo Gestione licenza o EULA.

Fare clic su **<Scegli pacchetto>** per selezionare un pacchetto del programma di installazione dall'archivio oppure specificare un URL del pacchetto. Verrà visualizzato un elenco di pacchetti disponibili tra cui scegliere il prodotto ESET che si desidera installare (ad esempio, ESET Endpoint Security). Selezionare il pacchetto del programma di installazione desiderato, quindi fare clic su **OK**. Se si desidera specificare l'URL del pacchetto di installazione, è necessario digitarlo o copiarlo e incollarlo nel campo di testo (non utilizzare un URL che richiede l'autenticazione).

NOTA: si tenga presente che sia il server sia l'agente necessitano dell'accesso a Internet per poter accedere all'archivio ed eseguire l'installazione. Se non si dispone di un accesso a Internet, è possibile installare il software client localmente.

Se necessario, è possibile specificare i Parametri di installazione, altrimenti lasciare questo campo vuoto. Per eseguire un riavvio automatico del computer client al termine dell'installazione, selezionare la casella di controllo accanto a **Riavvia automaticamente se necessario**. In alternativa, è possibile lasciare deselezionata questa opzione e lasciare a un altro utente la decisione di riavviare il computer client.



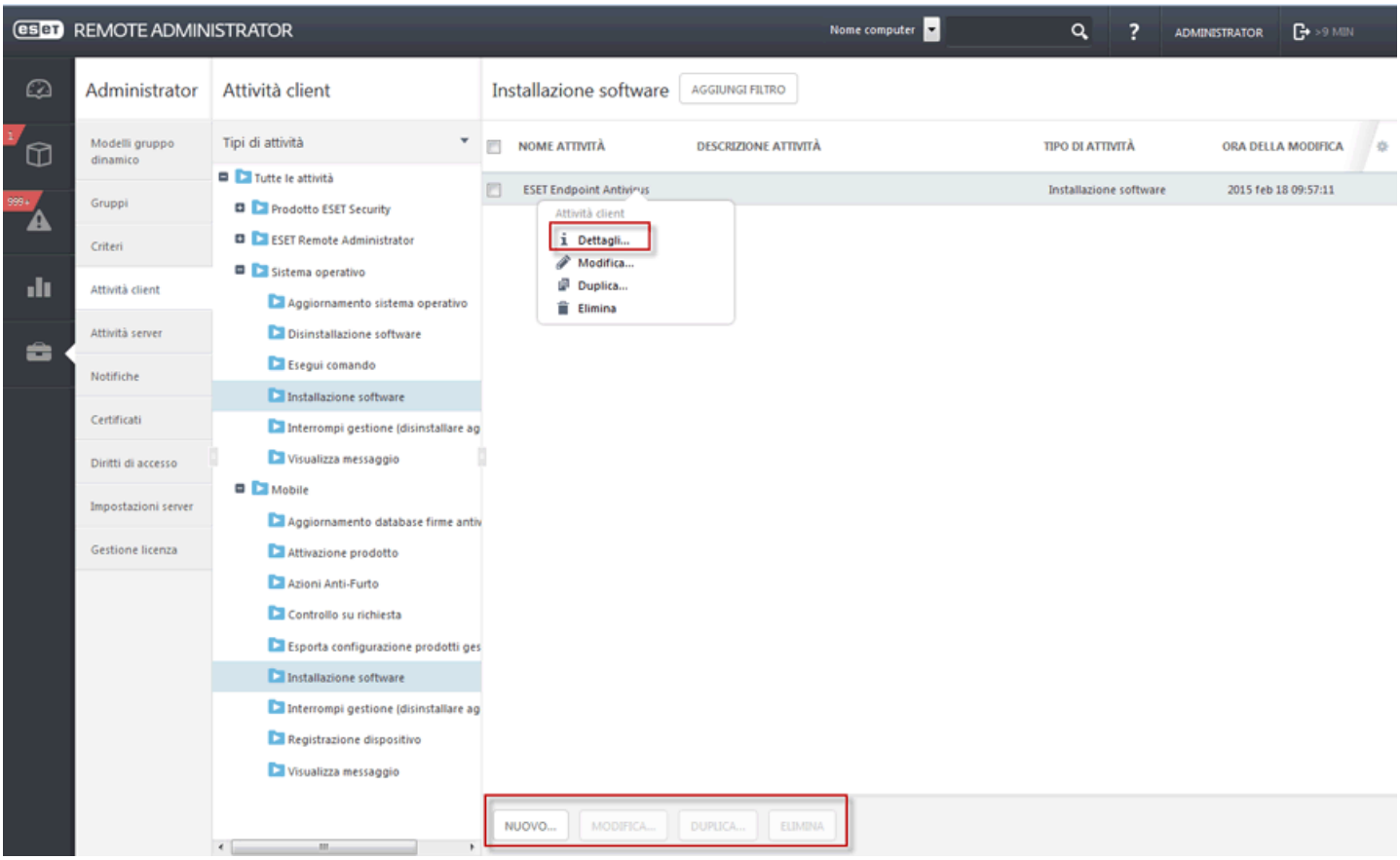
Riepilogo

Rivedere il riepilogo delle impostazioni configurate e fare clic su **Fine**. L'attività è stata creata e verrà inviata a/i client.

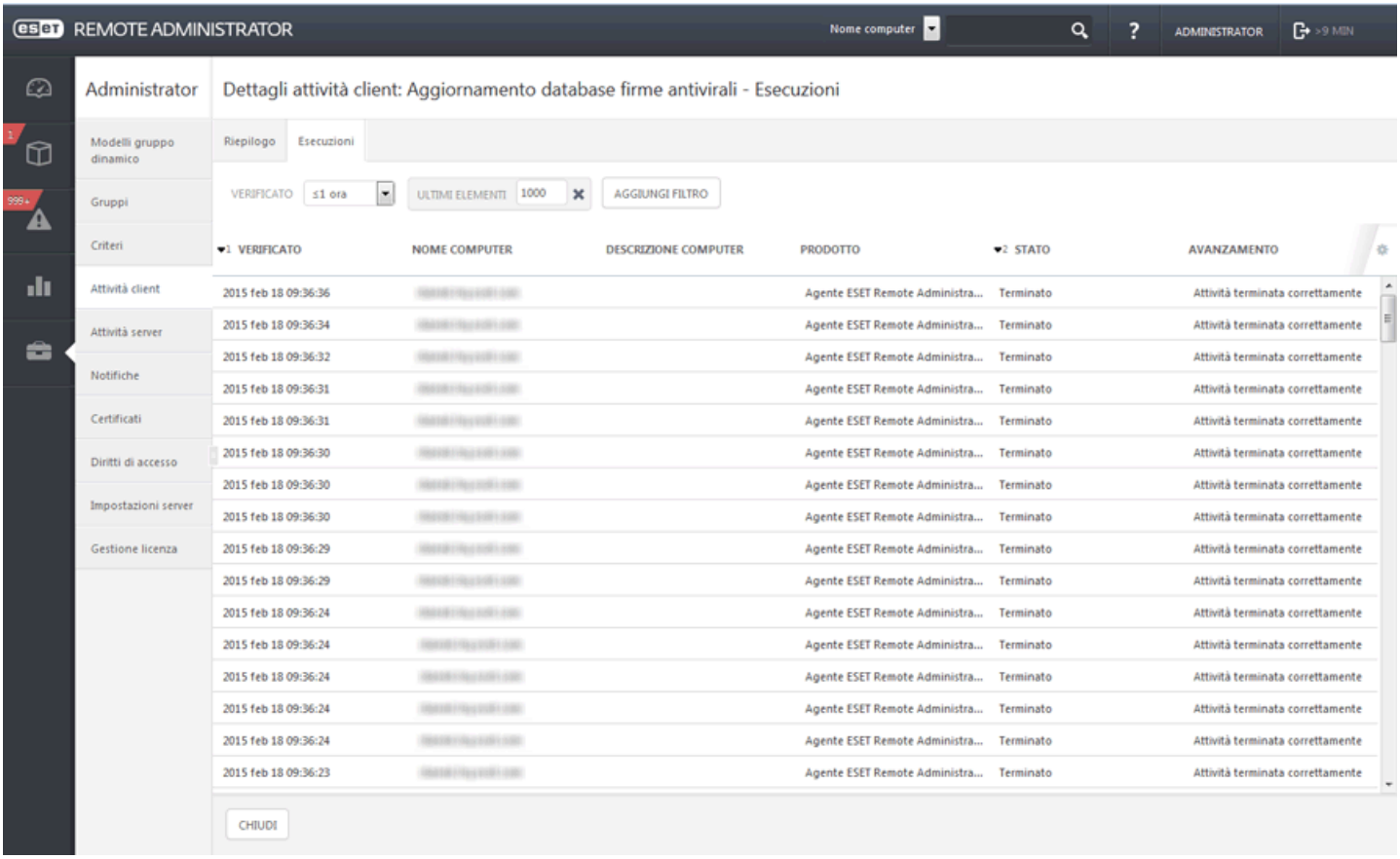
6.1.3.2 Gestisci attività client

È possibile utilizzare l'opzione Attività client per gestire i client e i relativi prodotti di protezione. Sono disponibili una serie di attività predefinite che dovrebbero contemplare gli utilizzi più comuni oppure è possibile creare attività personalizzate con impostazioni specifiche.

- È possibile utilizzare l'opzione **Modifica** per modificare le attività esistenti e crearne di nuove. La modifica delle attività esistenti risulta un'operazione utile quando è necessario apportare solo modifiche di lieve entità. Per creare attività più univoche, potrebbe essere preferibile creare una nuova attività da zero.
- **Duplica:** verrà aggiunta una nuova attività client in base all'attività selezionata. Per l'attività duplicata è necessario immettere un nuovo nome.
- **Elimina**: consente di rimuovere completamente le attività selezionate.



- **Dettagli...** : consente di visualizzare la configurazione dell'attività, il **Riepilogo** e le **Esecuzioni** dell'attività. (Verificatosi, Nome computer, Prodotto, Stato e avanzamento).



NOTA: quando si installa un prodotto di una versione precedente, nel rapporto dell'attività cliente viene visualizzata l'informazione Attività consegnata al prodotto gestito.

6.1.3.2.1 Controllo su richiesta

L'attività **Controllo su richiesta** consente all'utente di eseguire un controllo manuale sul computer client (diverso da un controllo pianificato periodico).

Arresta al termine del controllo: se si seleziona questa casella di controllo, il computer si arresterà al termine del controllo.

Profilo di controllo - È possibile selezionare il profilo desiderato dal menu a discesa:

- **Controllo approfondito**: profilo predefinito sul client, che viene configurato in modo da garantire il massimo livello di controllo e che consente di eseguire una verifica dell'intero sistema richiedendo, però, più tempo e l'utilizzo di un maggior numero di risorse.
- **Controllo intelligente -** La funzione Controllo intelligente consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio del Controllo intelligente consiste nella facilità di utilizzo e nel fatto che non è richiesta una configurazione di controllo dettagliata. Il Controllo intelligente consente di effettuare un controllo di tutti i file presenti nelle unità locali, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito.
- **Controlla dal menu contestuale**: questa opzione permette di controllare un cliente utilizzando un profilo di controllo predefinito. È possibile personalizzare le destinazioni di controllo.
- **Profilo personalizzato**: consente all'utente di specificare parametri di controllo quali destinazioni e metodi di controllo. Il vantaggio di un Controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni su profili di controllo definiti dall'utente che facilitano la ripetizione del controllo attraverso l'utilizzo degli stessi parametri. Prima di eseguire l'attività con l'opzione del profilo personalizzato, è necessario creare un profilo. Dopo aver selezionato un profilo personalizzato dal menu a discesa, immettere il nome esatto del profilo nel campo **Profilo personalizzato**.

Pulizia

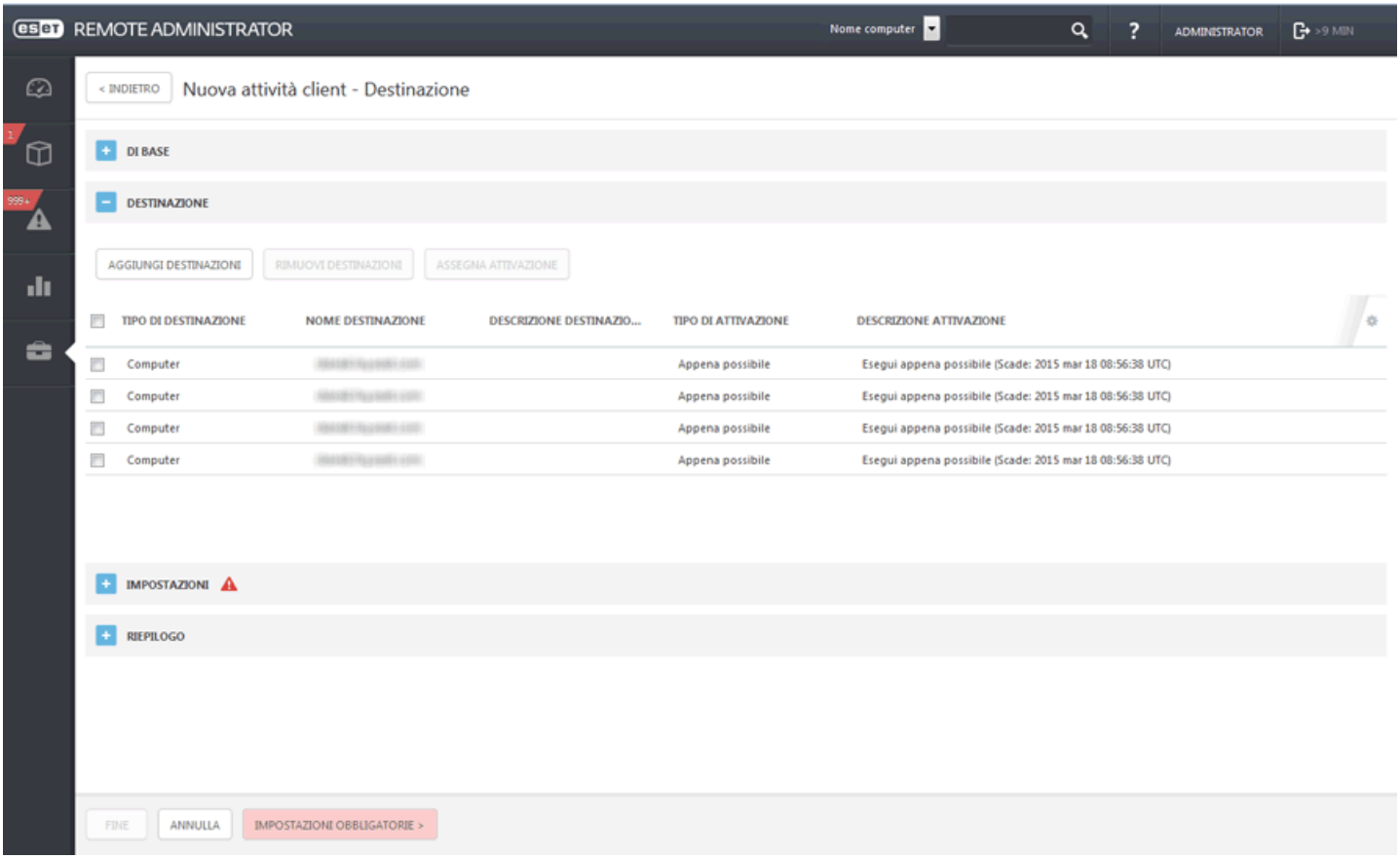
Per impostazione predefinita, è selezionata l'opzione **Controllo con pulizia**. Ciò significa che, in caso di individuazione di oggetti infetti, questi vengono puliti automaticamente. Qualora ciò non fosse possibile, tali oggetti verranno messi in quarantena.

Destinazioni di controllo

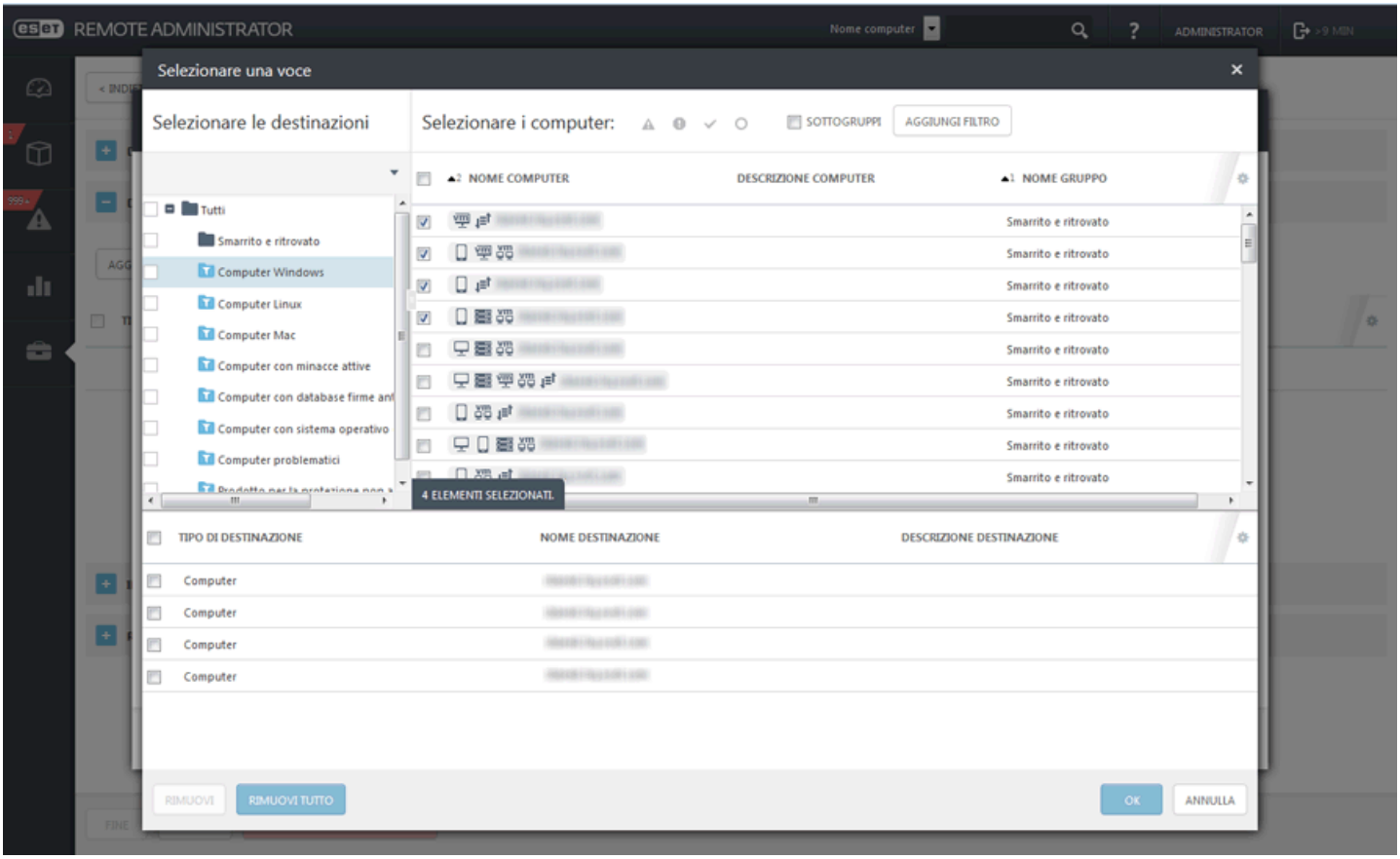
Questa opzione, selezionata anch'essa per impostazione predefinita, consente di controllare tutte le destinazioni specificate nel profilo di controllo. Qualora sia disattivata, è necessario specificare manualmente le destinazioni di controllo nel campo **Aggiungi destinazione**. Digitare la destinazione di controllo nel campo di testo e fare clic su **Aggiungi**. La destinazione verrà visualizzata nel campo Destinazioni di controllo sottostante.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Riepilogo

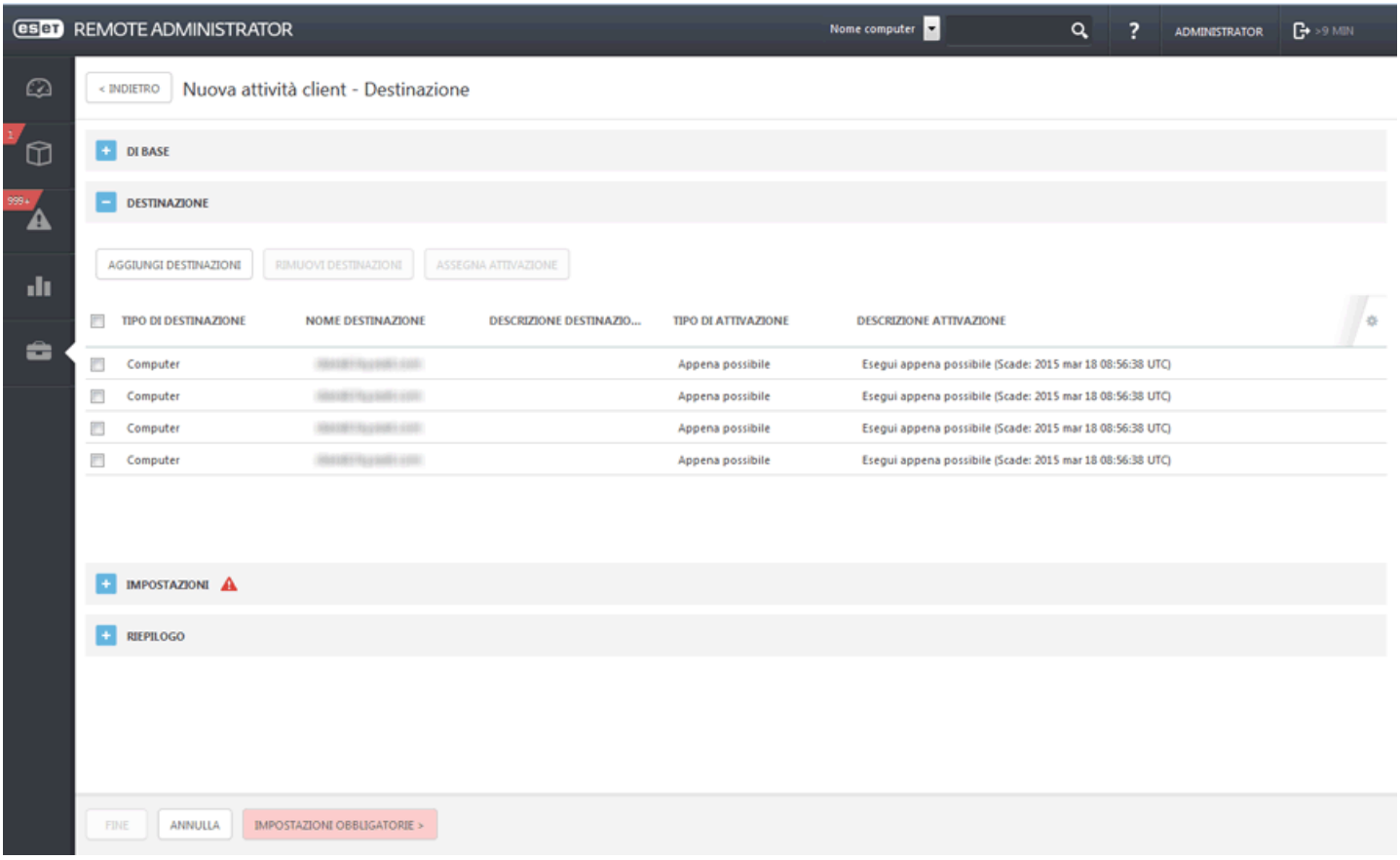
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.2 Aggiornamento sistema operativo

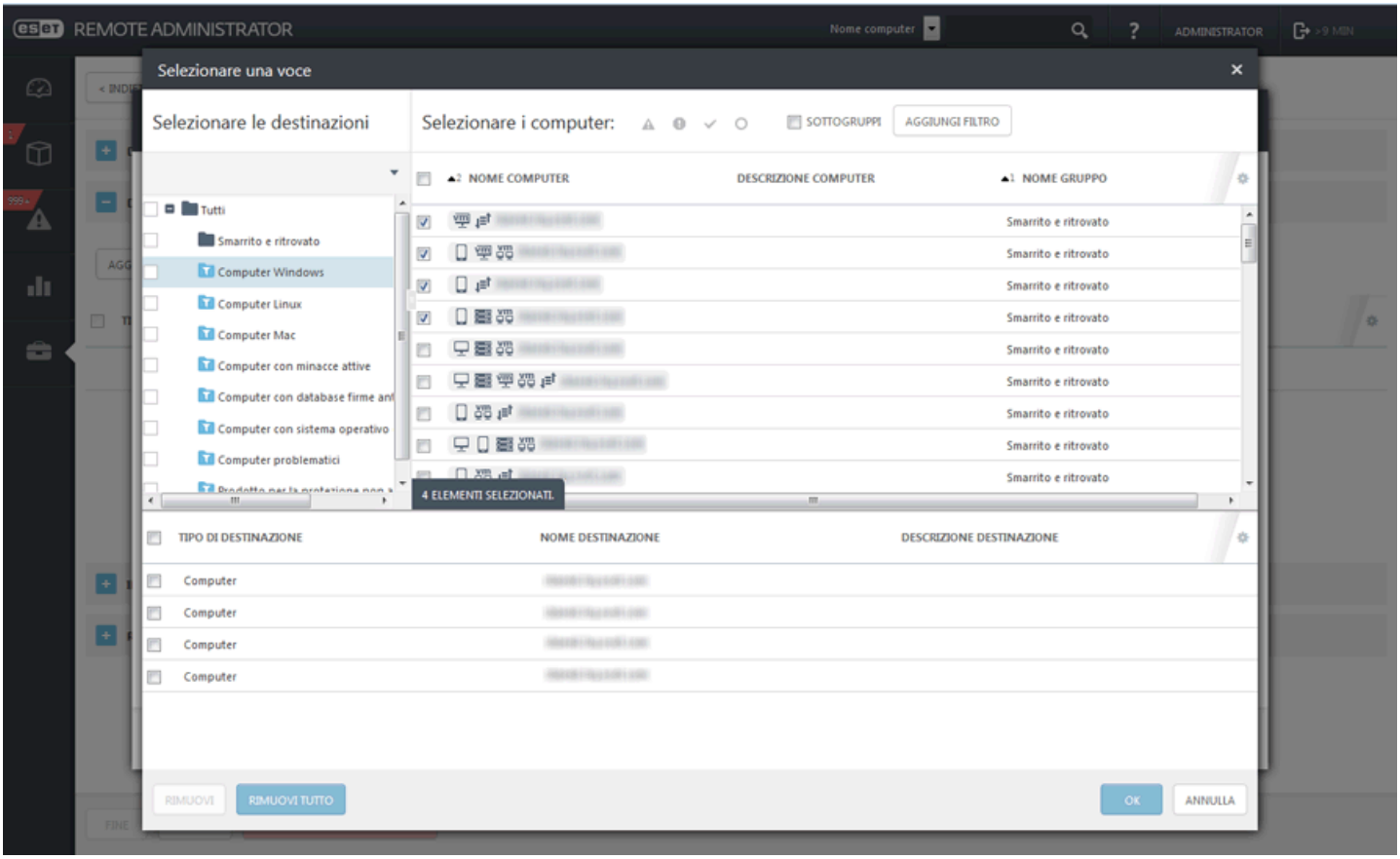
L'attività **Aggiornamento sistema** viene utilizzata per aggiornare il sistema operativo del computer client. Questa attività attiva l'aggiornamento dei sistemi operativi Windows, Mac e Linux.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Consenti riavvio**: questa opzione si applica solo ai sistemi operativi Windows e determina il riavvio del computer client in seguito all'installazione di un aggiornamento.

Riepilogo

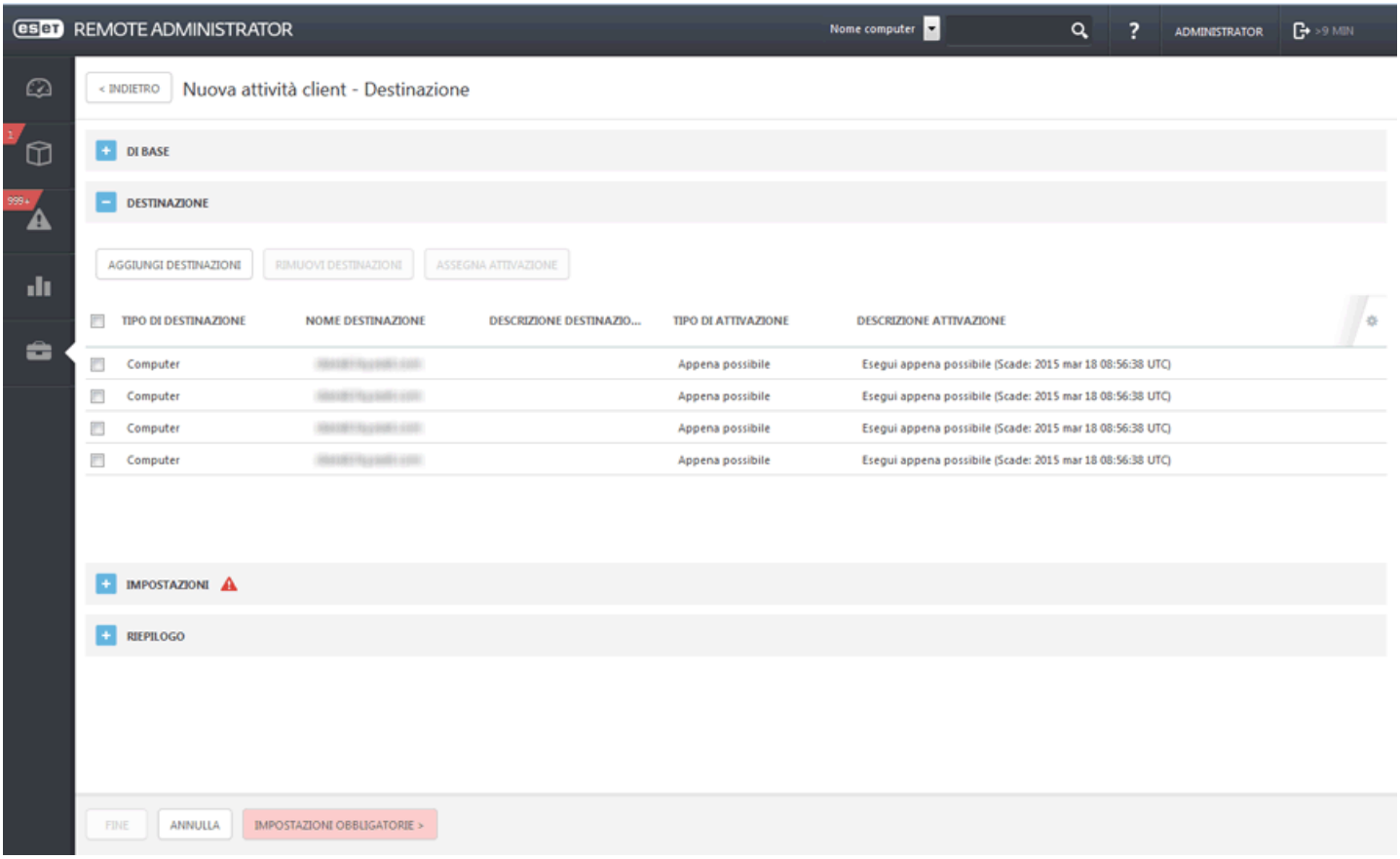
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.3 Gestione quarantena

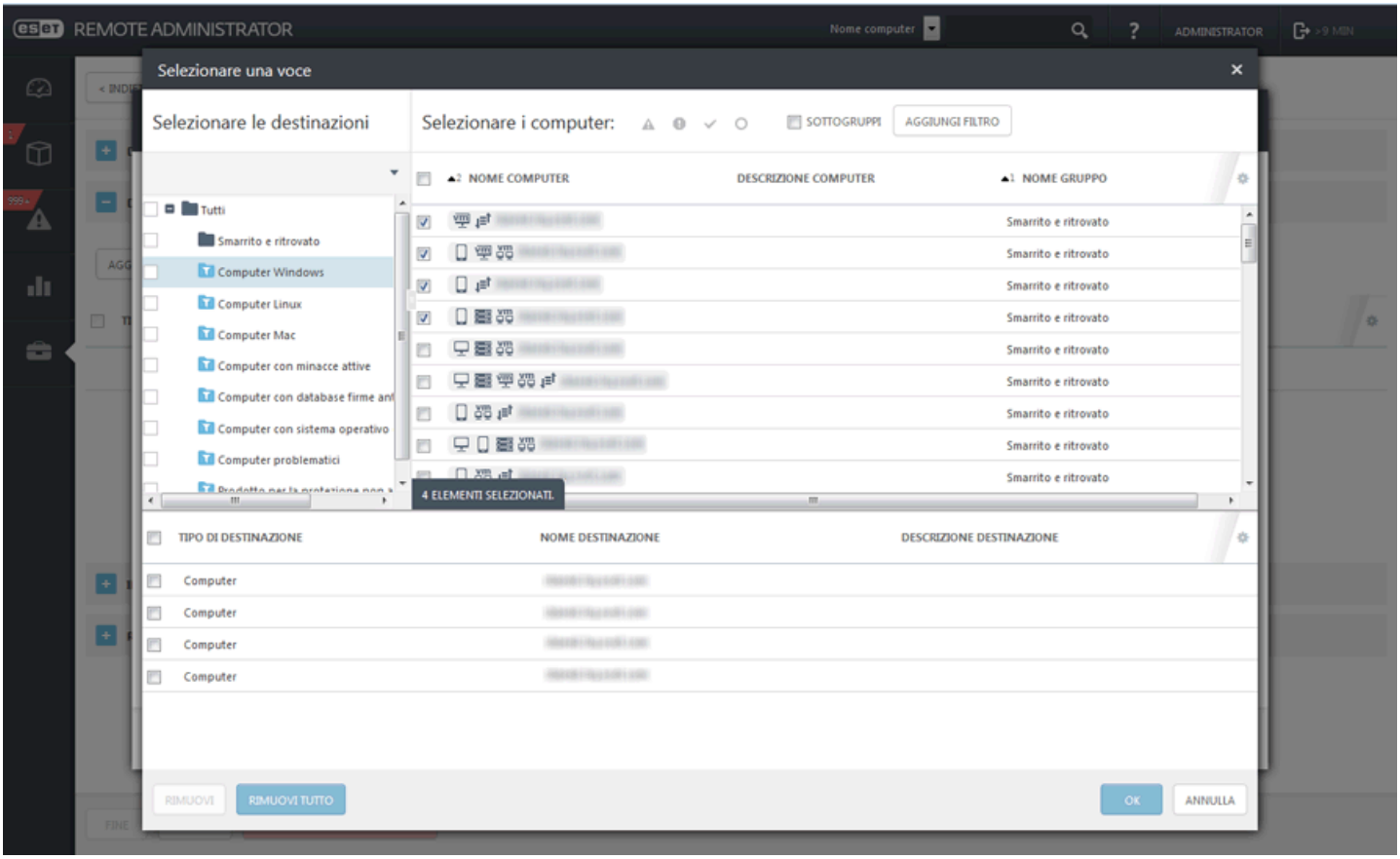
L'attività **Gestione quarantena** viene utilizzata per gestire oggetti infetti o sospetti trovati durante il controllo nella quarantena del server ERA.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

Impostazioni gestione quarantena

- **Azione**: selezionare l'azione da intraprendere con l'oggetto in quarantena.

Ripristina oggetto (ripristina la posizione originale dell'oggetto che verrà tuttavia controllato e messo nuovamente in quarantena in caso di persistenza dei motivi)
Ripristina oggetto ed escludi in futuro (ripristina la posizione originale dell'oggetto che non verrà messo nuovamente in quarantena).
Elimina oggetto (elimina completamente l'oggetto).

- **Tipo di filtro**: filtra gli oggetti della quarantena in base ai criteri definiti di seguito. Impostazione basata sulla stringa Hash dell'oggetto o sulle Condizioni.

Impostazioni filtro hash

Aggiungere gli elementi hash nel campo. È possibile aggiungere solo oggetti conosciuti come, ad esempio, quelli già messi in quarantena.

Impostazioni filtro condizionali

- **Verificato da/a**: definisce l'intervallo temporale in cui l'oggetto è stato messo in quarantena.
- **Dimensione minima/massima (byte)**: definisce l'intervallo di dimensioni dell'oggetto in quarantena (in byte).
- **Nome minaccia**: selezionare una minaccia dall'elenco di elementi in quarantena.
- **Nome oggetto**: selezionare un oggetto dall'elenco di elementi in quarantena.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

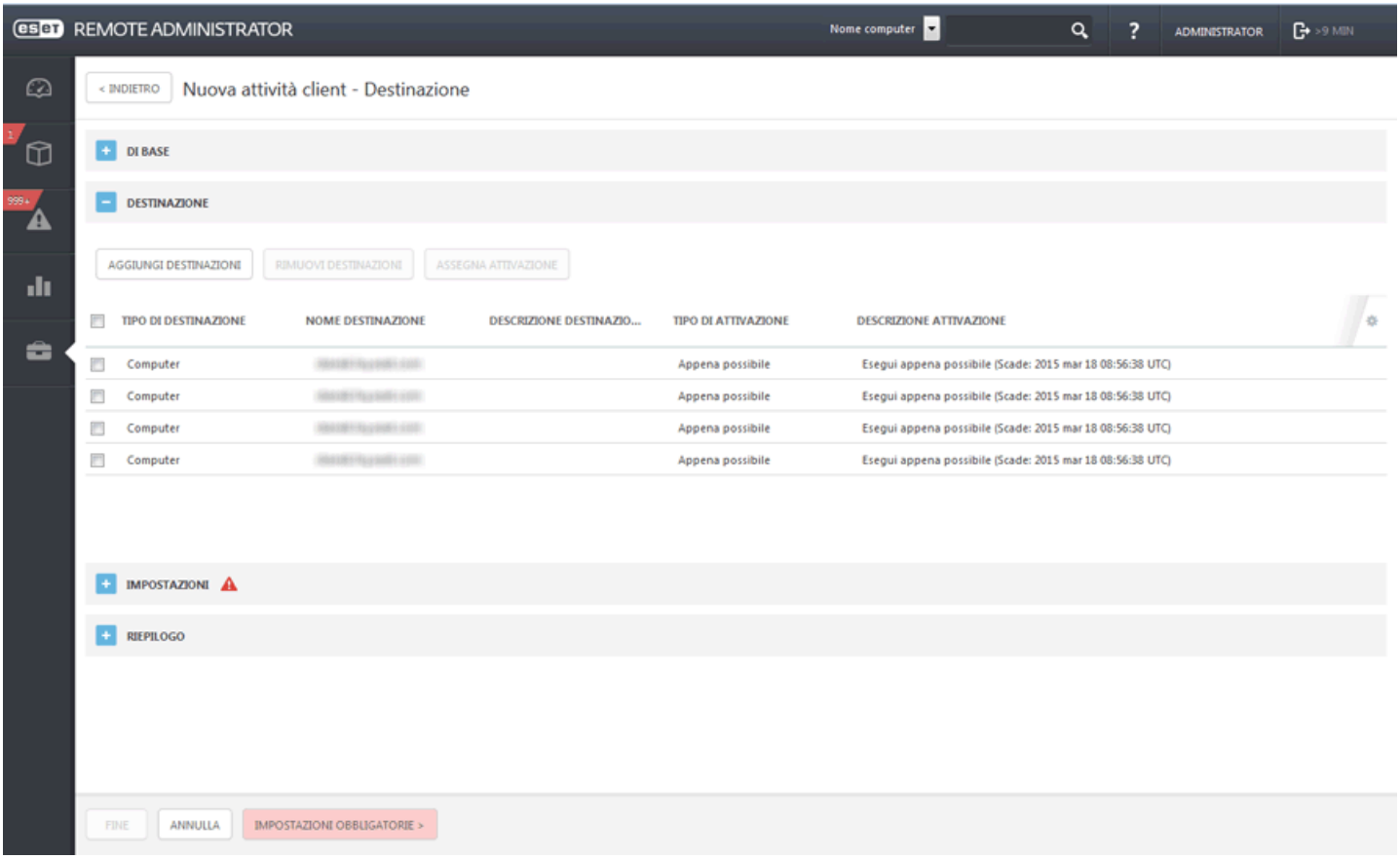
6.1.3.2.4 Reimposta database Rogue Detection Sensor

L'attività **Reimposta database Rogue Detection Sensor** viene utilizzata per reimpostare la cache di ricerca di RD Sensor. In seguito all'eliminazione della cache da parte dell'attività, i risultati di ricerca verranno memorizzati nuovamente. Questa attività non rimuove i computer rilevati. ed è utile nel caso in cui i computer rilevati rimangano nella cache e non vengano segnalati al server.

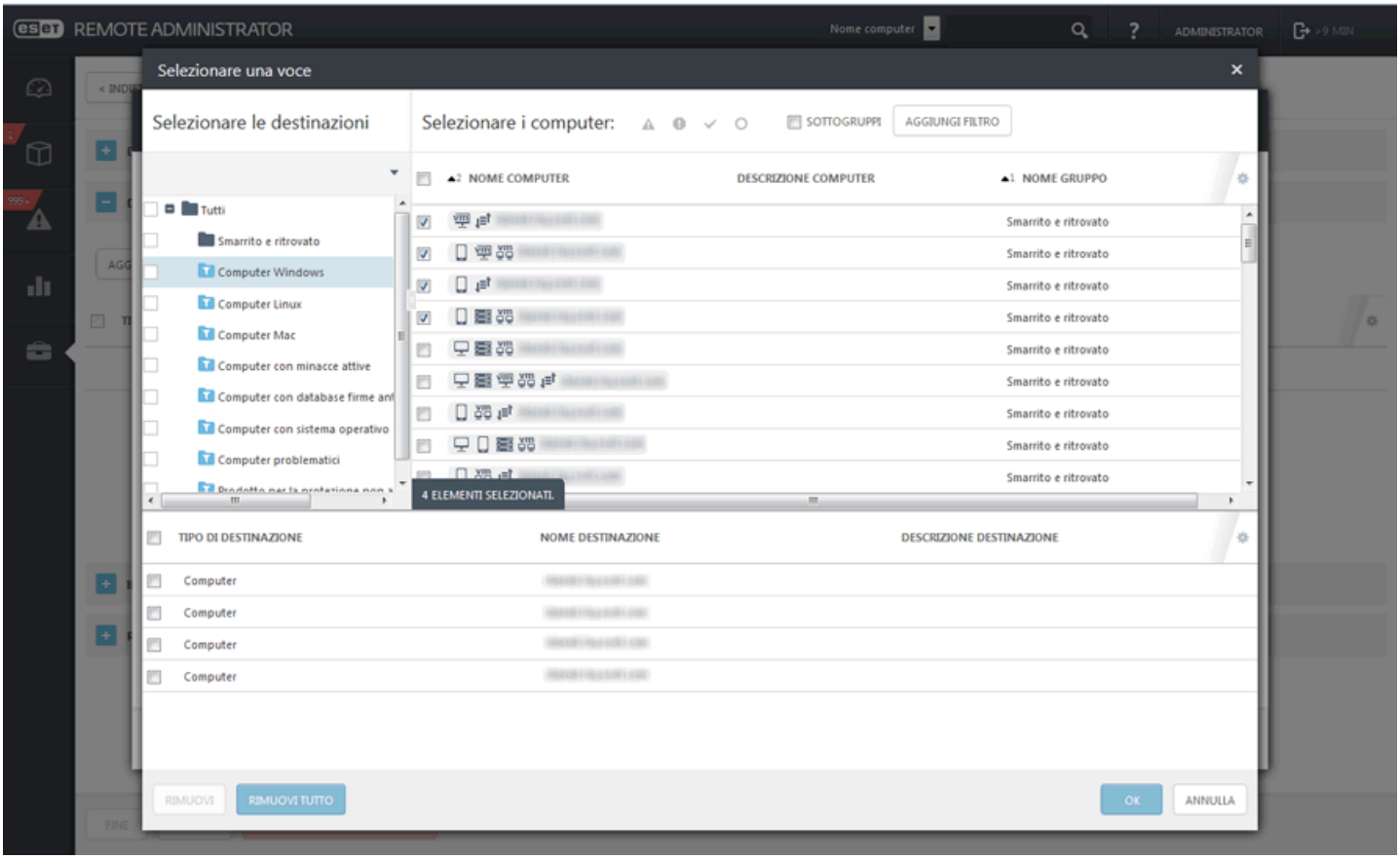
NOTA: non sono disponibili impostazioni per questa attività.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Riepilogo

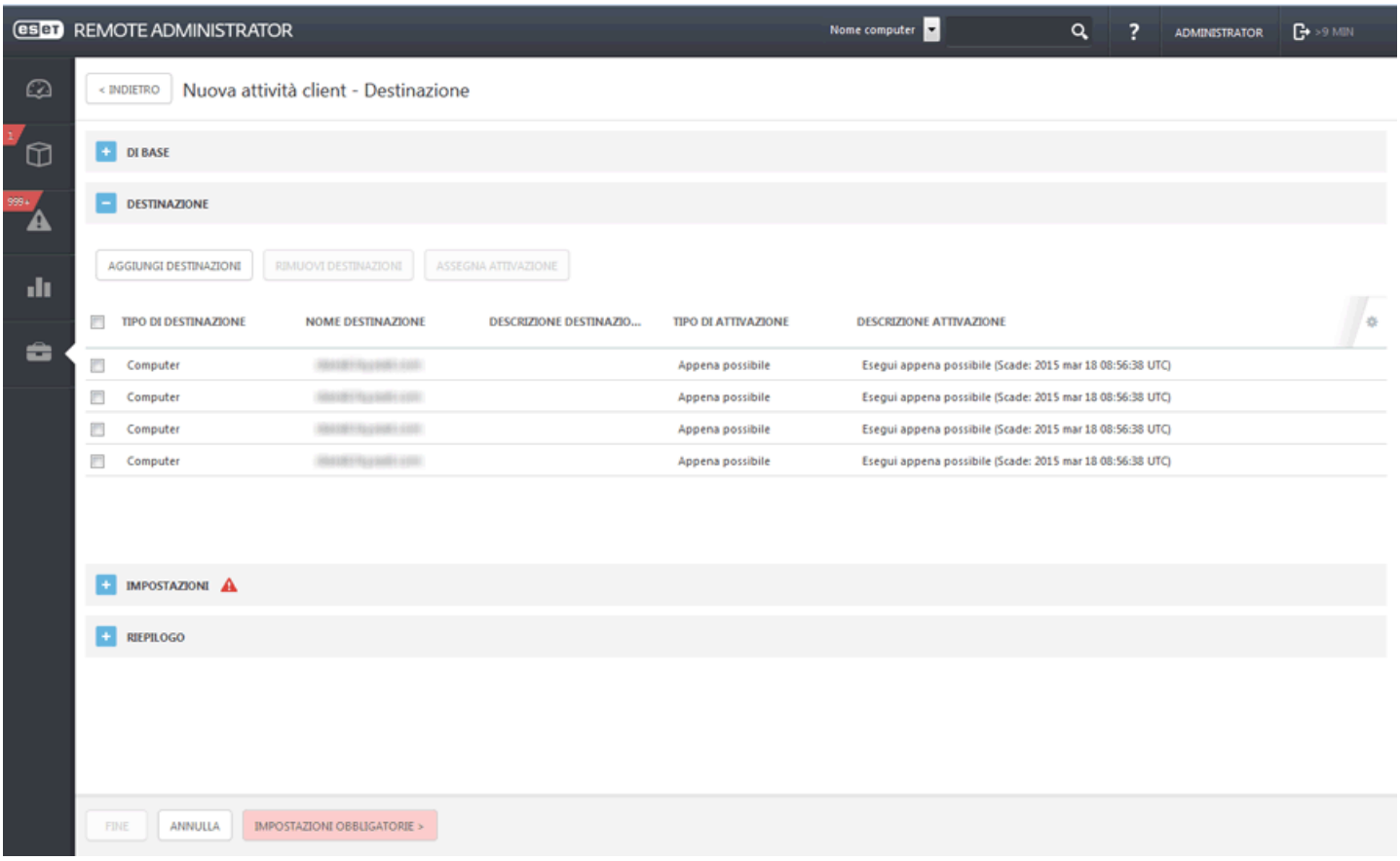
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.5 Aggiornamento componenti amministratore remoto

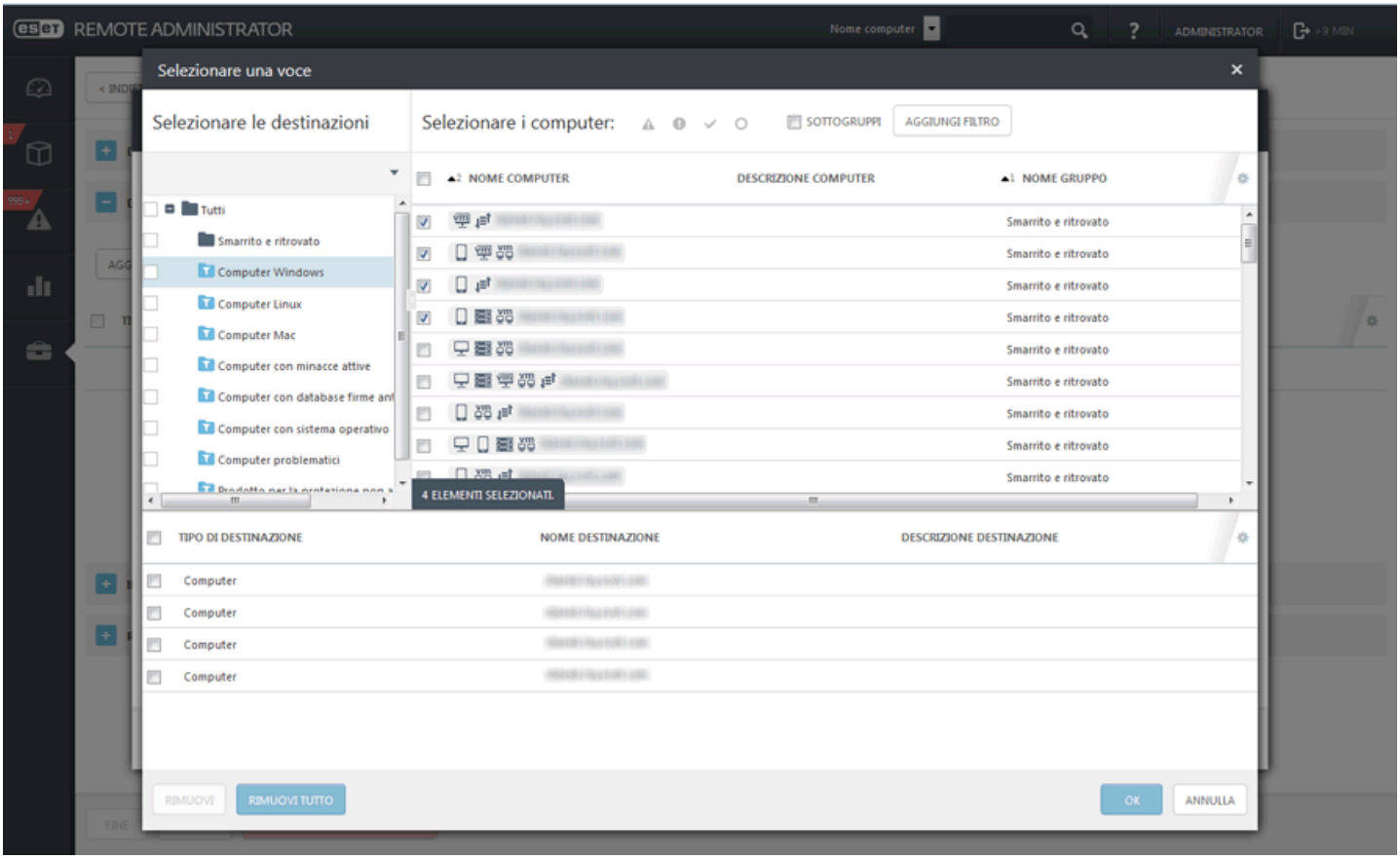
L'attività **Aggiornamento componenti amministratore remoto** viene utilizzata per aggiornare i componenti principali di ERA (agente, proxy, server ed MDM) installati su un client alla versione compatibile con uno specifico server ERA (server di riferimento).

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Server di riferimento amministratore remoto**: selezionare la versione del server ERA dall'elenco. Tutti i componenti ERA verranno aggiornati alle versioni compatibili con il server selezionato.
- **Riavvia automaticamente se necessario**: è possibile forzare un riavvio del sistema operativo client qualora richiesto dal processo di installazione.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

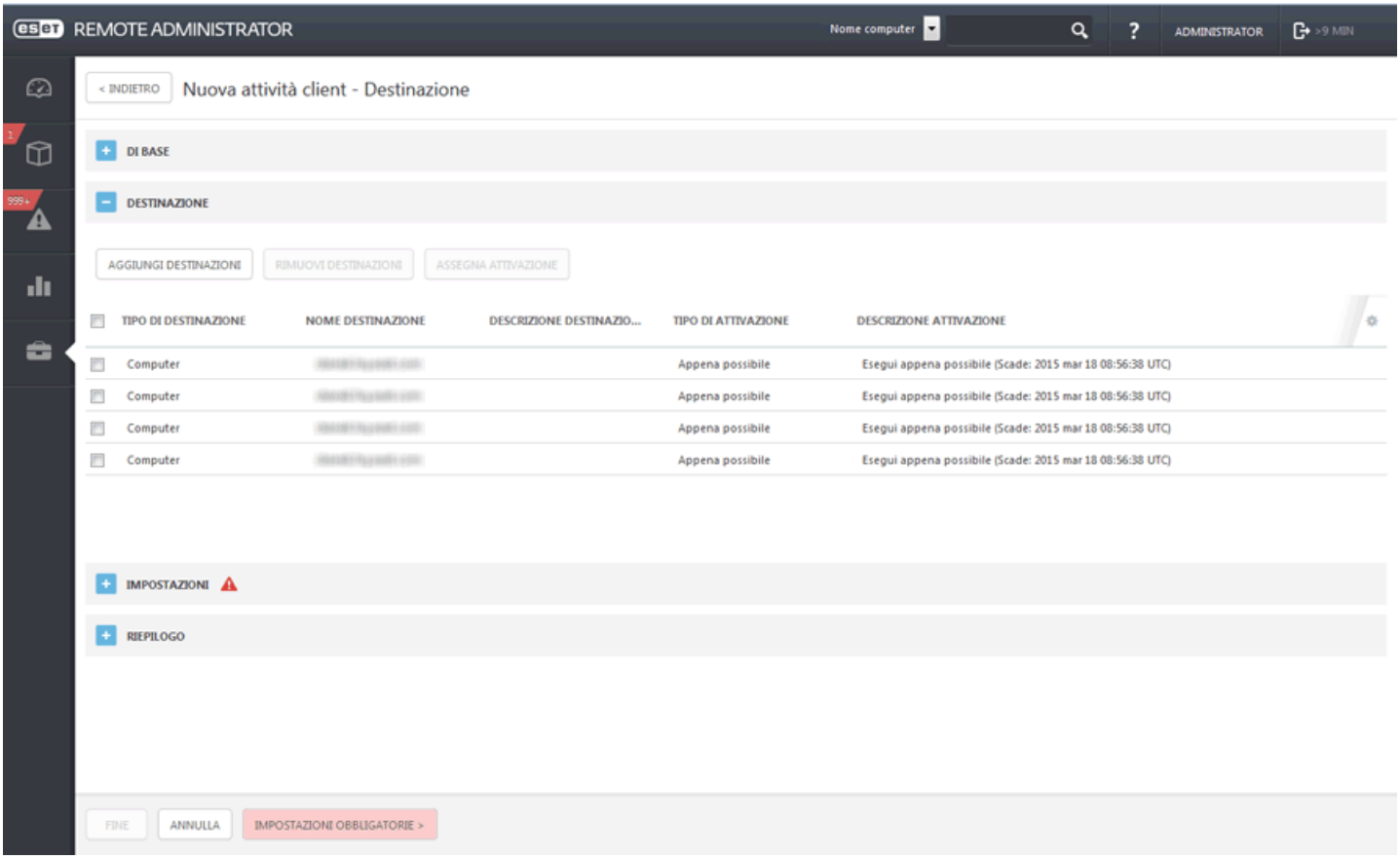
6.1.3.2.6 Reimposta agente clonato

L'attività **Reimposta agente clonato** può essere utilizzata per distribuire l'agente ESET nella rete attraverso un'immagine predefinita. Gli agenti clonati presentano lo stesso SID e ciò potrebbe causare alcuni problemi (presenza di più di un agente con lo stesso SID) per la cui risoluzione è necessario utilizzare l'attività Reimposta agente clonato che consente di reimpostare il SID e di assegnare agli agenti un'identità univoca.

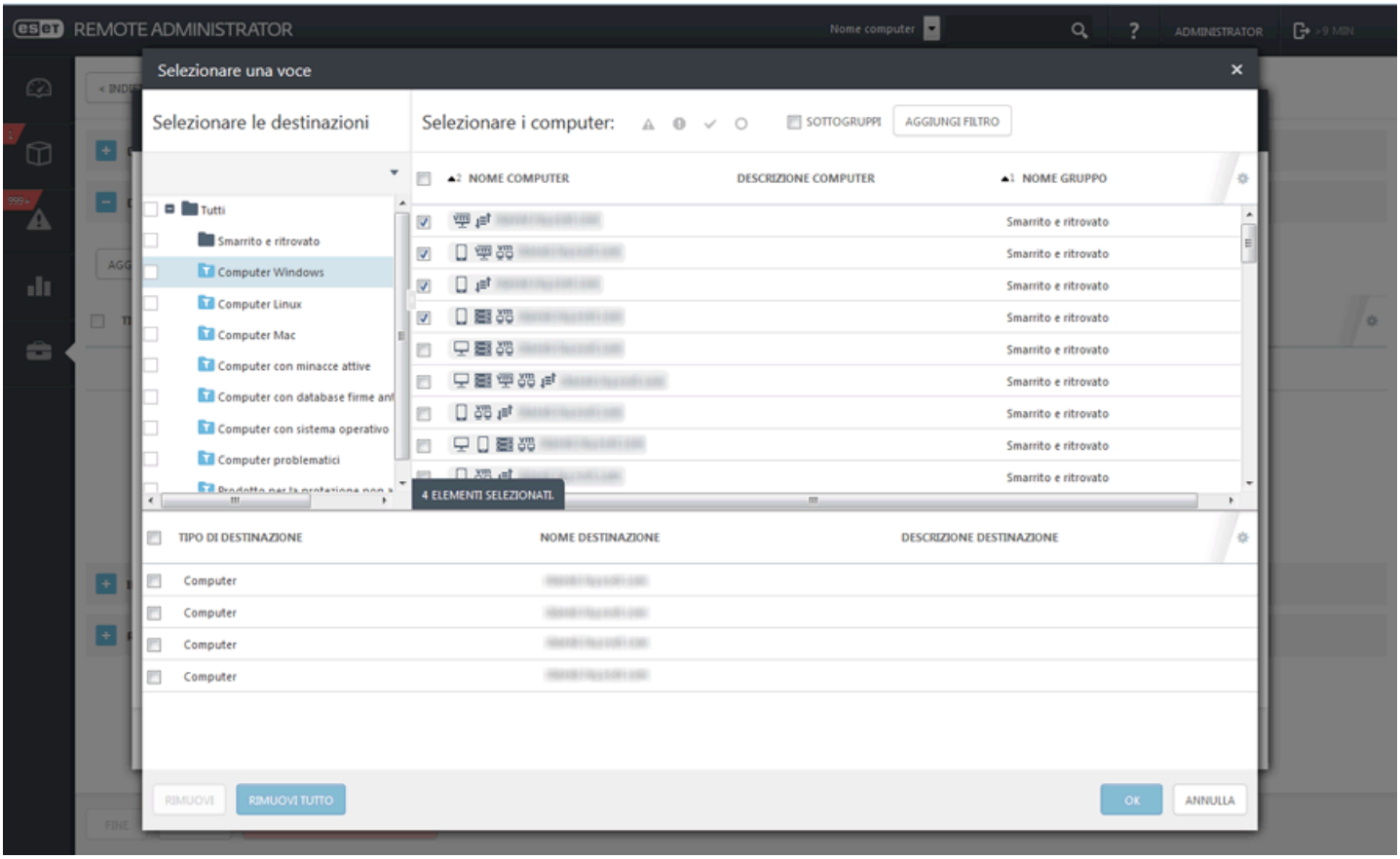
NOTA: non sono disponibili impostazioni per questa attività.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Riepilogo

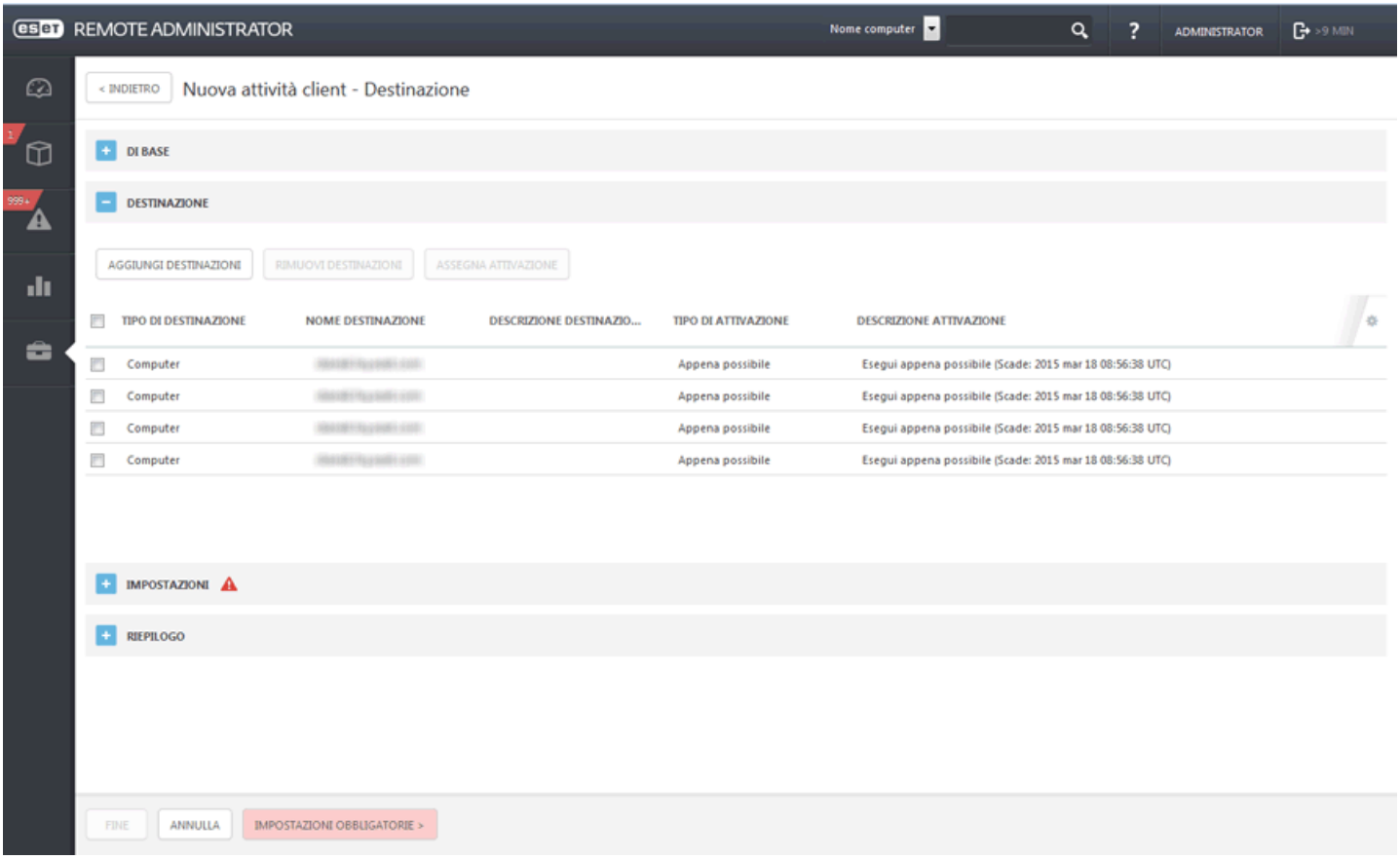
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.7 Esegui comando

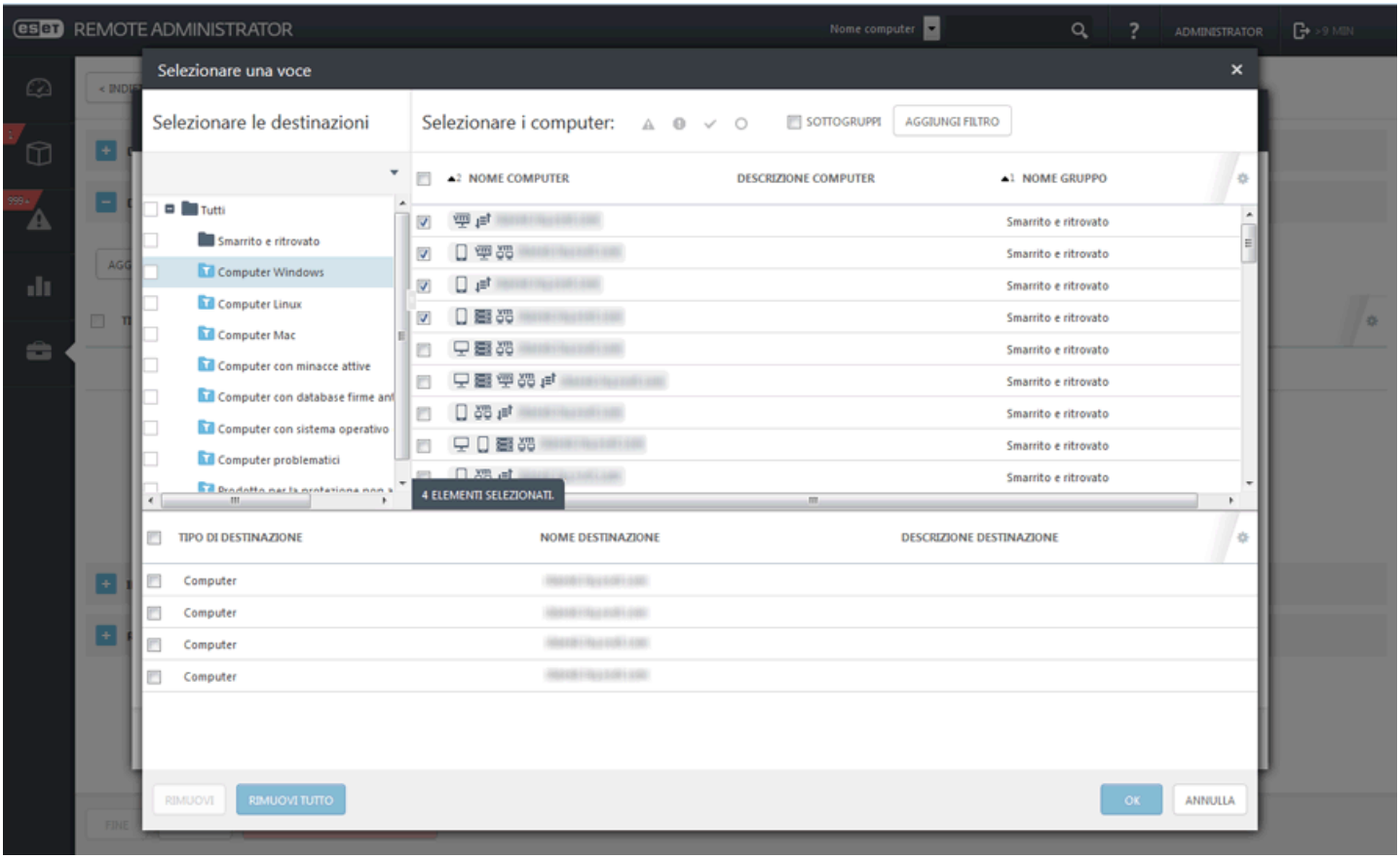
L'attività **Esegui comando** può essere utilizzata per eseguire specifiche istruzioni della riga di comando sul client. L'amministratore specifica l'inserimento della riga di comando da eseguire.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Riga di comando da eseguire**: inserire una riga di comando che si desidera eseguire su uno o più client.
- **Directory di lavoro**: inserire una directory in cui verrà eseguita la riga di comando di cui sopra.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

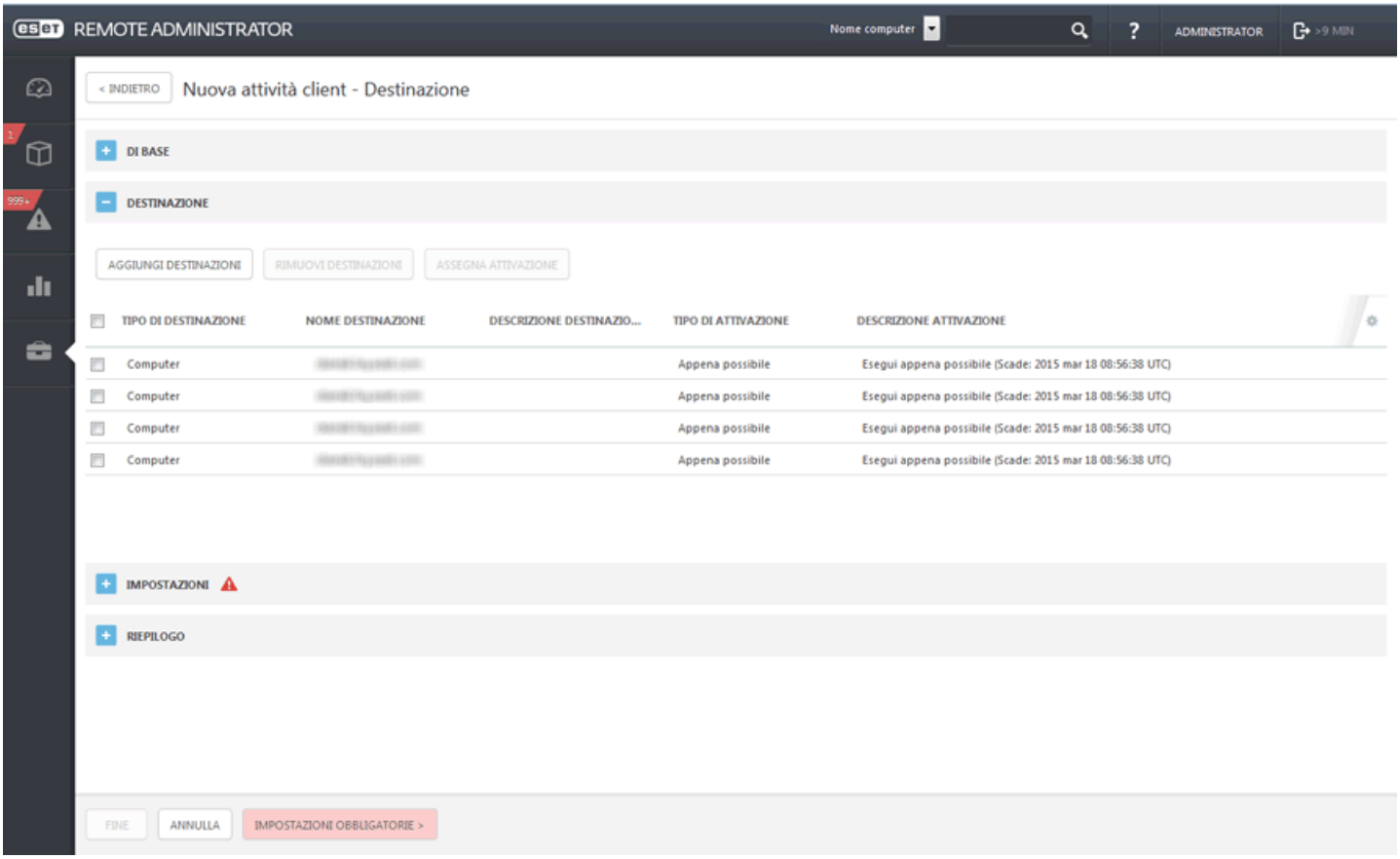
6.1.3.2.8 Esegui script SysInspector

L'attività **Esegui script SysInspector** viene utilizzata per rimuovere oggetti indesiderati dal sistema. Prima di utilizzare questa attività, è necessario esportare uno **Script SysInspector** da ESET SysInspector. Dopo aver esportato lo script, è possibile contrassegnare gli oggetti che si desidera rimuovere ed eseguire lo script con i dati modificati: a questo punto, gli oggetti contrassegnati verranno eliminati.

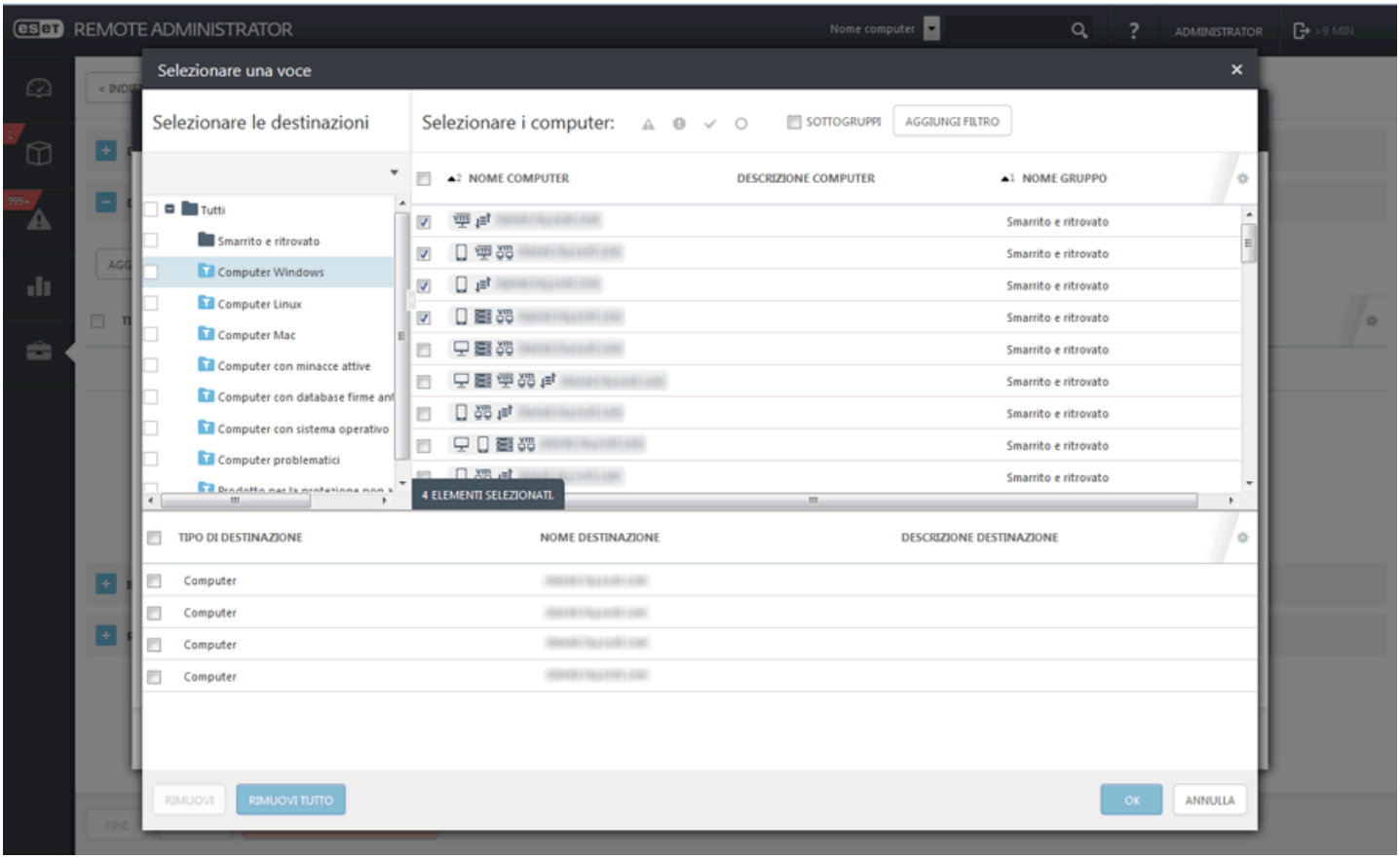
NOTA: al termine dell'attività è possibile controllare i risultati in un rapporto.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Script SysInspector**: fare clic su **Sfoglia** per accedere allo script di servizio. Lo script di servizio deve essere creato prima dell'esecuzione dell'attività.
- **Azione**: è possibile **Caricare** o **Scaricare** uno script dalla console ERA.

Riepilogo

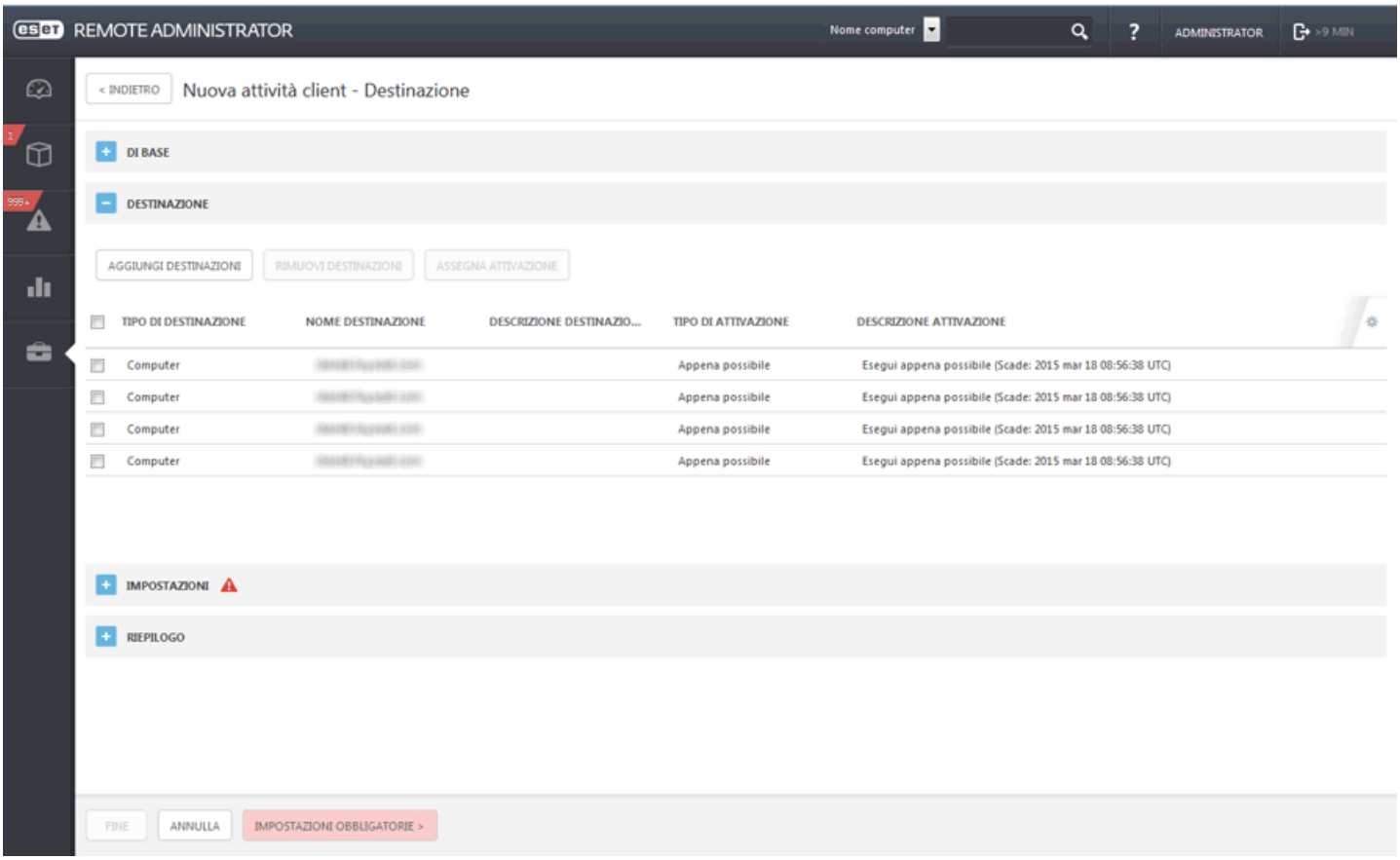
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.9 Installazione software

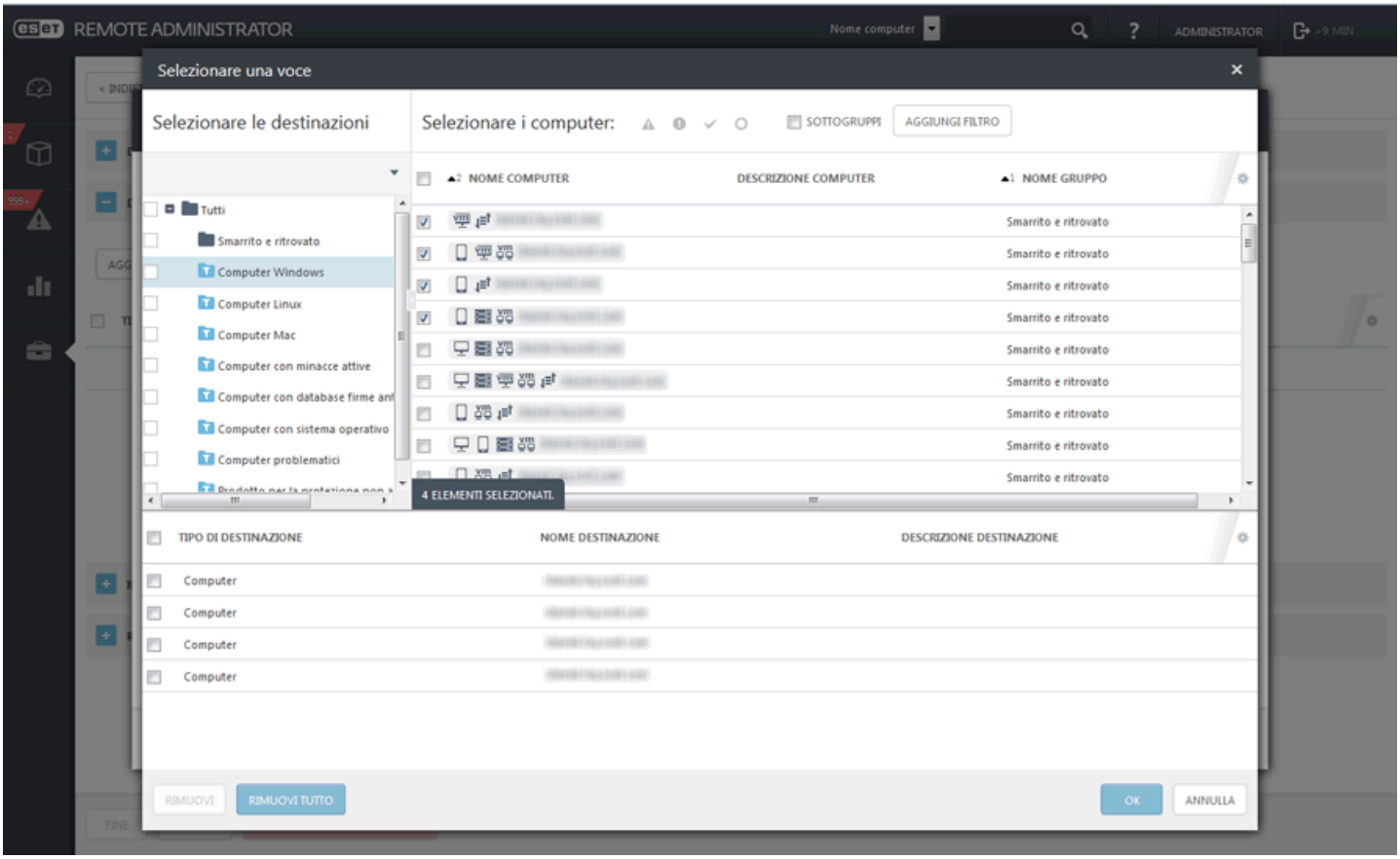
L'attività **Installazione software** viene utilizzata per l'installazione del software sui computer client. Sebbene questo strumento sia concepito principalmente per l'installazione di prodotti ESET, è possibile utilizzarlo anche per l'installazione di qualsiasi altro software. Utilizzare le istruzioni che seguono oppure guardare il video illustrativo della Knowledge Base.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

Fare clic su **<Scegliere licenza ESET>** e selezionare la licenza appropriata per il prodotto installato nell'elenco di licenze disponibili. Se d'accordo, selezionare la casella di controllo accanto a **Accetto i termini del Contratto di licenza per l'utente finale relativo alla richiesta**. Per ulteriori informazioni, consultare il capitolo Gestione licenza o EULA.

Fare clic su **<Scegli pacchetto>** per selezionare un pacchetto del programma di installazione dall'archivio oppure specificare un URL del pacchetto. Verrà visualizzato un elenco di pacchetti disponibili tra cui scegliere il prodotto ESET che si desidera installare (ad esempio, ESET Endpoint Security). Selezionare il pacchetto del programma di installazione desiderato, quindi fare clic su **OK**. Se si desidera specificare l'URL del pacchetto di installazione, è necessario digitarlo o copiarlo e incollarlo nel campo di testo (non utilizzare un URL che richiede l'autenticazione).

NOTA: si tenga presente che sia il server sia l'agente necessitano dell'accesso a Internet per poter accedere all'archivio ed eseguire l'installazione. Se non si dispone di un accesso a Internet, è possibile installare il software client localmente.

Se necessario, è possibile specificare i Parametri di installazione, altrimenti lasciare questo campo vuoto. Per eseguire un riavvio automatico del computer client al termine dell'installazione, selezionare la casella di controllo accanto a **Riavvia automaticamente se necessario**. In alternativa, è possibile lasciare deselezionata questa opzione e lasciare a un altro utente la decisione di riavviare il computer client.

Riepilogo

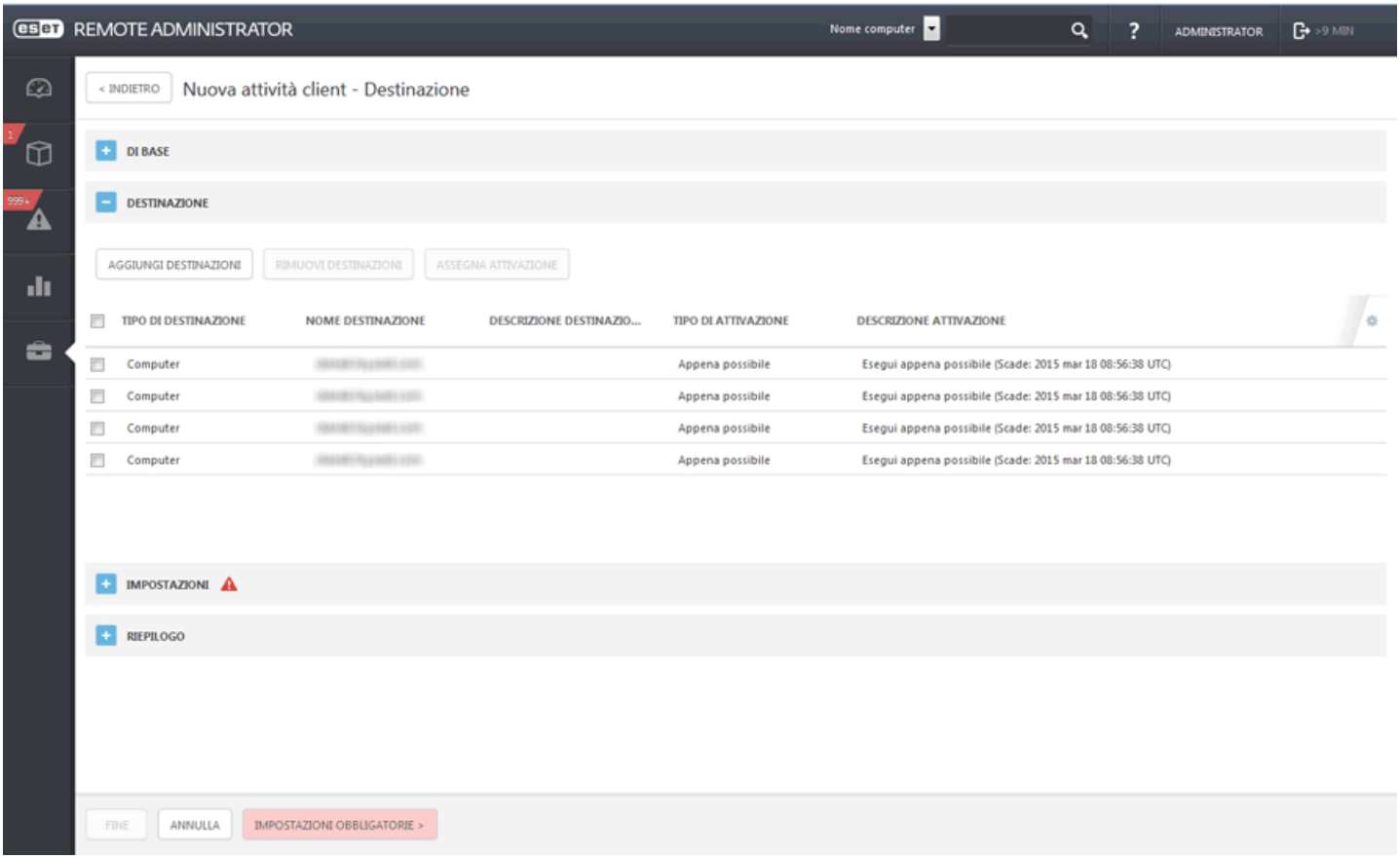
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.10 Disinstallazione software

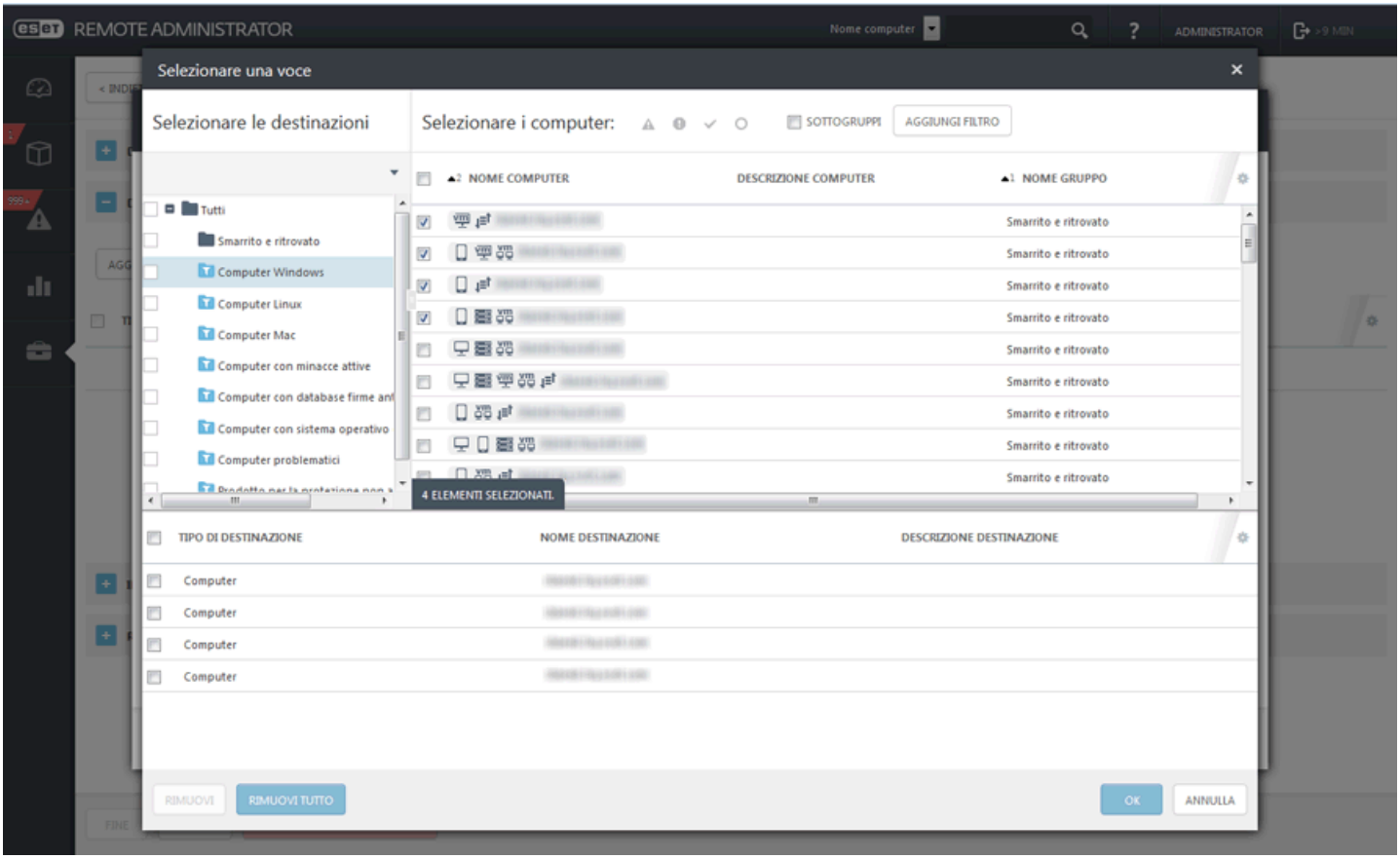
L'attività **Disinstallazione software** viene utilizzata per disinstallare i prodotti ESET dai client nel caso in cui non siano più desiderati o necessari. Se si sta disinstallando l'agente ERA, i prodotti ESET gestiti da questo agente potrebbero mantenere alcune impostazioni anche in seguito all'operazione.
Si consiglia di reimpostare alcune impostazioni predefinite (ad esempio protezione con password) attraverso l'utilizzo di un criterio prima che il dispositivo venga rimosso dalla gestione. Inoltre, tutte le attività in esecuzione sull'agente verranno abbandonate. In base alla replica, lo stato **In esecuzione**, **Terminata** o **Non riuscita** dell'attività potrebbe non essere visualizzato in modo accurato in ERA Web Console.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

Impostazioni disinstallazione software

- **Disinstalla - Applicazione dall'elenco:**

Nome pacchetto: selezionare un componente ERA o un prodotto di protezione client. Tutti i pacchetti installati su uno o più client selezionati vengono visualizzati in questo elenco.
Versione pacchetto: è possibile rimuovere una versione specifica (che, talvolta, potrebbe causare alcuni problemi) del pacchetto oppure disinstallare tutte le versioni di un pacchetto.
Riavvia automaticamente se necessario: è possibile forzare un riavvio del sistema operativo client qualora sia necessario ai fini della disinstallazione.

- **Disinstalla - software antivirus di terze parti (ideato con tecnologia OPSWAT):** per un elenco di software antivirus compatibili, consultare questo articolo della Knowledge Base. Questa rimozione differisce dalla disinstallazione **Aggiungi o rimuovi programmi**, in quanto utilizza metodi alternativi per la rimozione completa di software antivirus di terze parti, comprese eventuali voci di registro residue o altre tracce.

Seguire le istruzioni dettagliate contenute nell'articolo intitolato In che modo è possibile rimuovere software antivirus di terze parti dai computer client che utilizzano ESET Remote Administrator? (6.x) per inviare un'attività allo scopo di rimuovere un software antivirus di terze parti da computer client.

Riepilogo

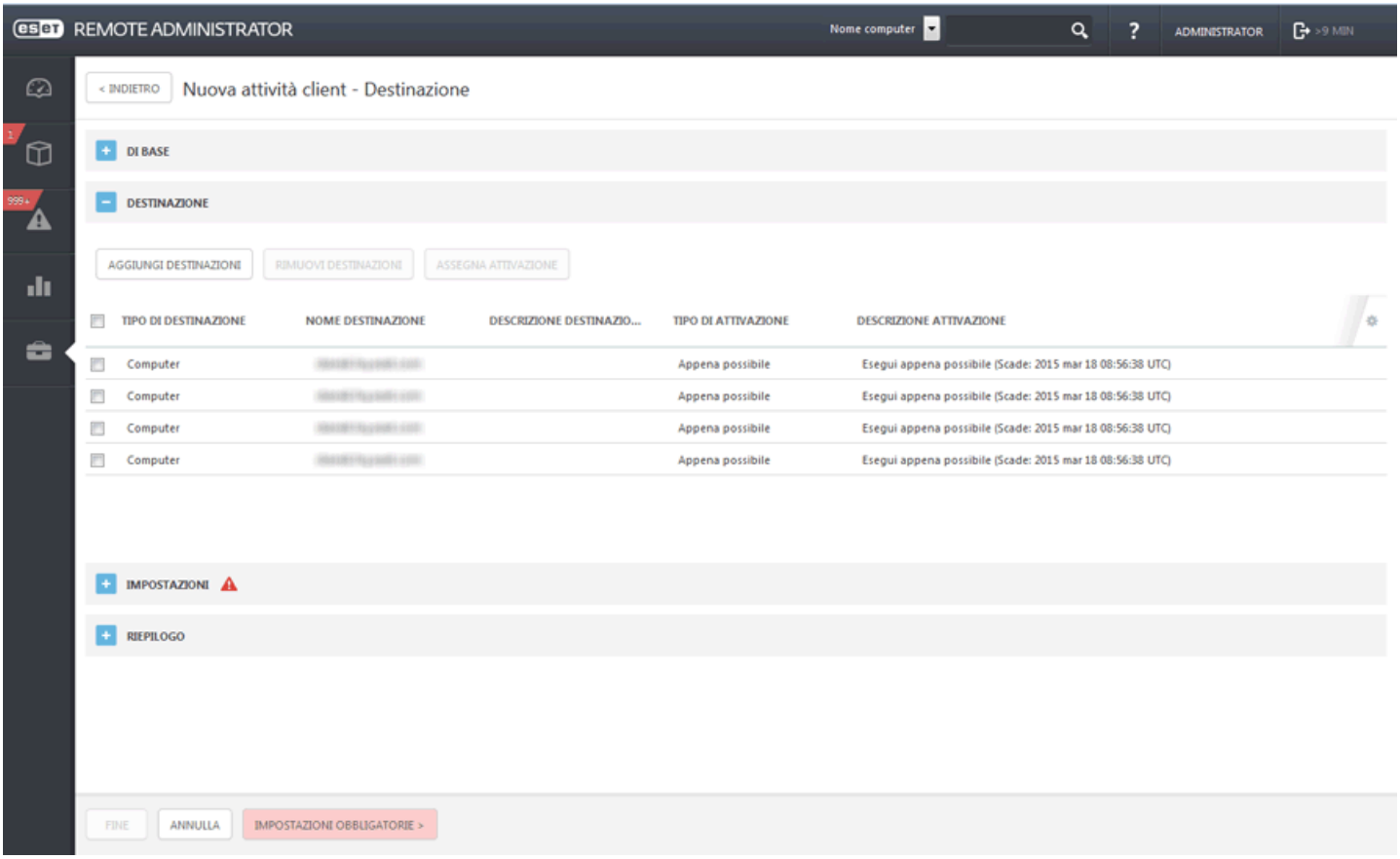
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.11 Attivazione prodotto

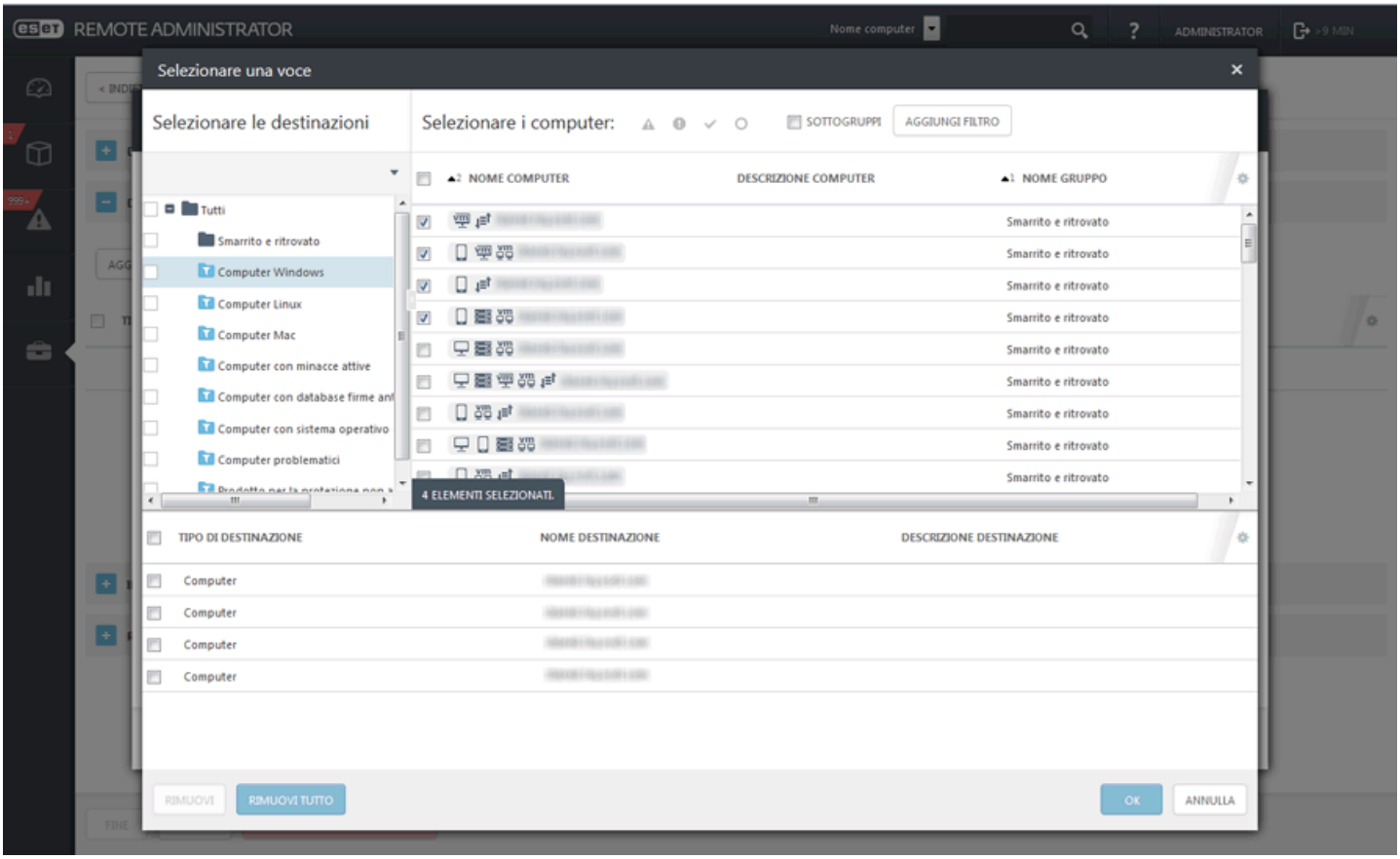
Per attivare un prodotto ESET su un computer client, attenersi ai seguenti passaggi:

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

Impostazioni attivazione prodotto: selezionare una licenza per il client dall'elenco. Verrà applicata ai prodotti già installati sul client.

Riepilogo

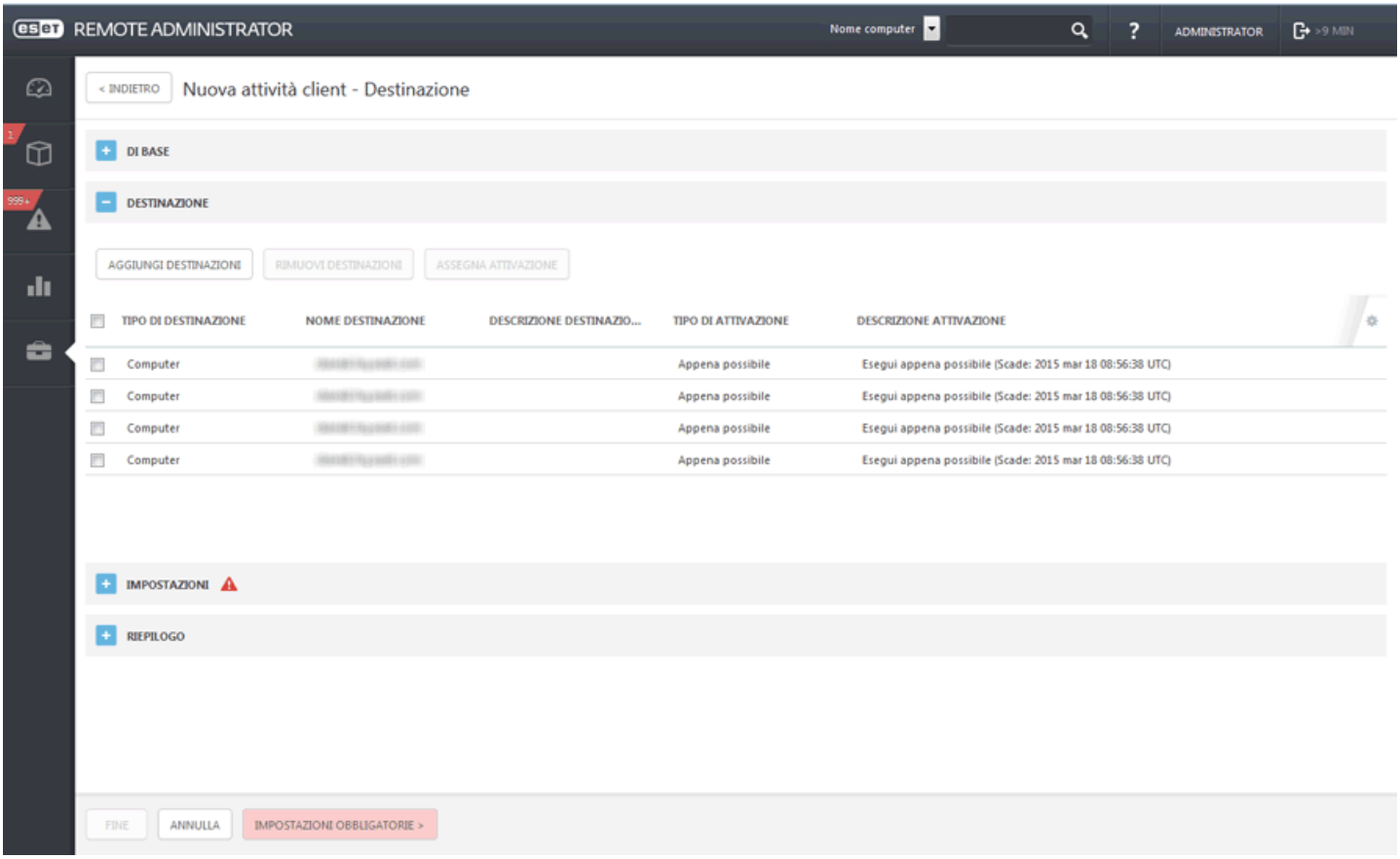
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.12 Richiesta rapporto SysInspector

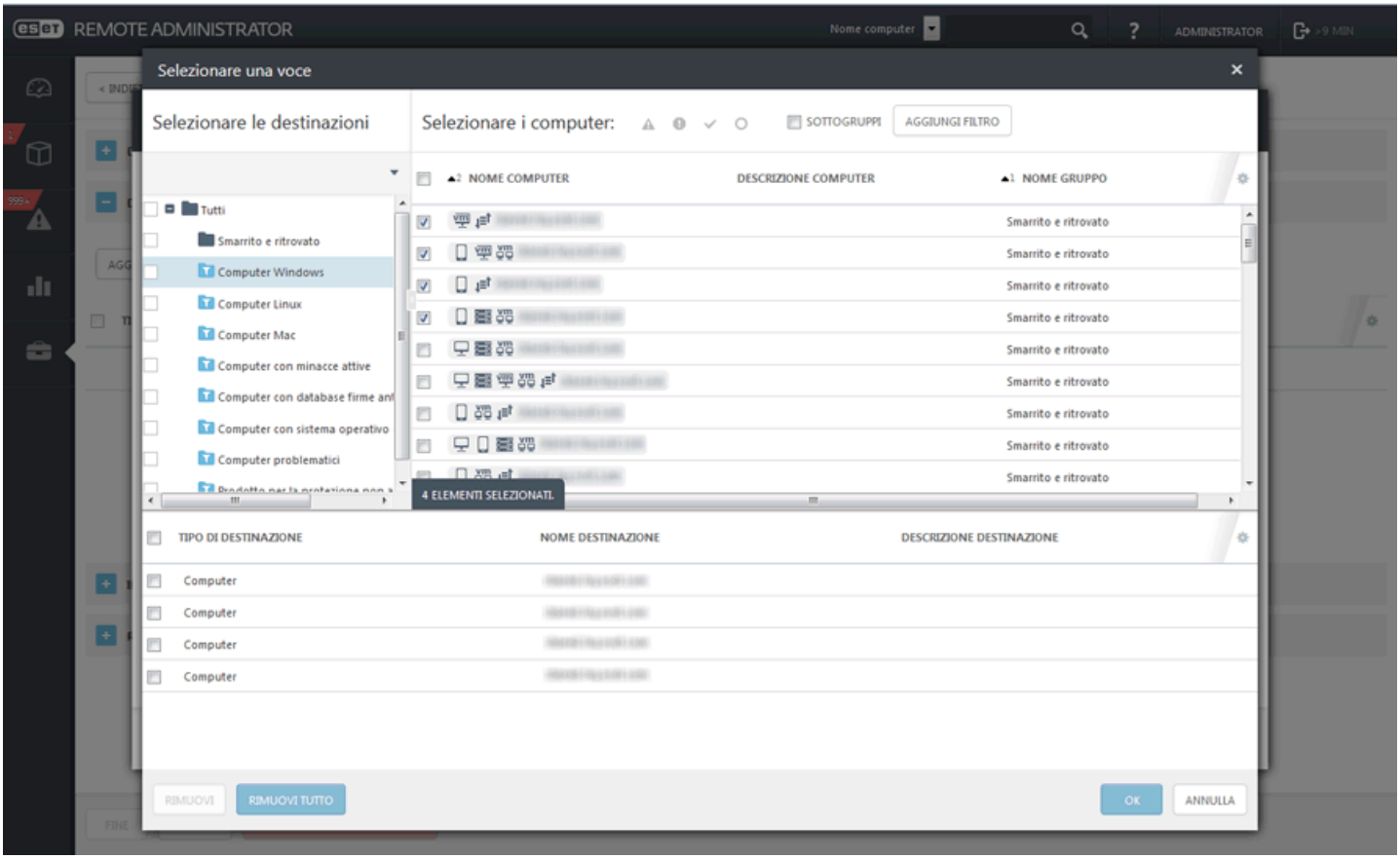
L'attività **Richiesta rapporto SysInspector** viene utilizzata per richiedere il rapporto SysInspector a un prodotto di protezione client che presenta questa funzione.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Archivia rapporto sul client**: selezionare questa opzione se si desidera archiviare il rapporto SysInspector sul client e sul server ERA. Ad esempio, se su un client è stato installato ESET Endpoint Security, il rapporto è solitamente archiviato in *C:\Programmi\ESET\ESET Endpoint Antivirus\SysInspector*.
- **Includi confronto con l'ultimo snapshot prima di un momento specificato**: consente all'utente di confrontare il rapporto generato con i rapporti relativi a uno specifico periodo di tempo antecedente al record. È possibile utilizzare le informazioni relative al confronto per individuare le differenze e le modifiche sul client.

Riepilogo

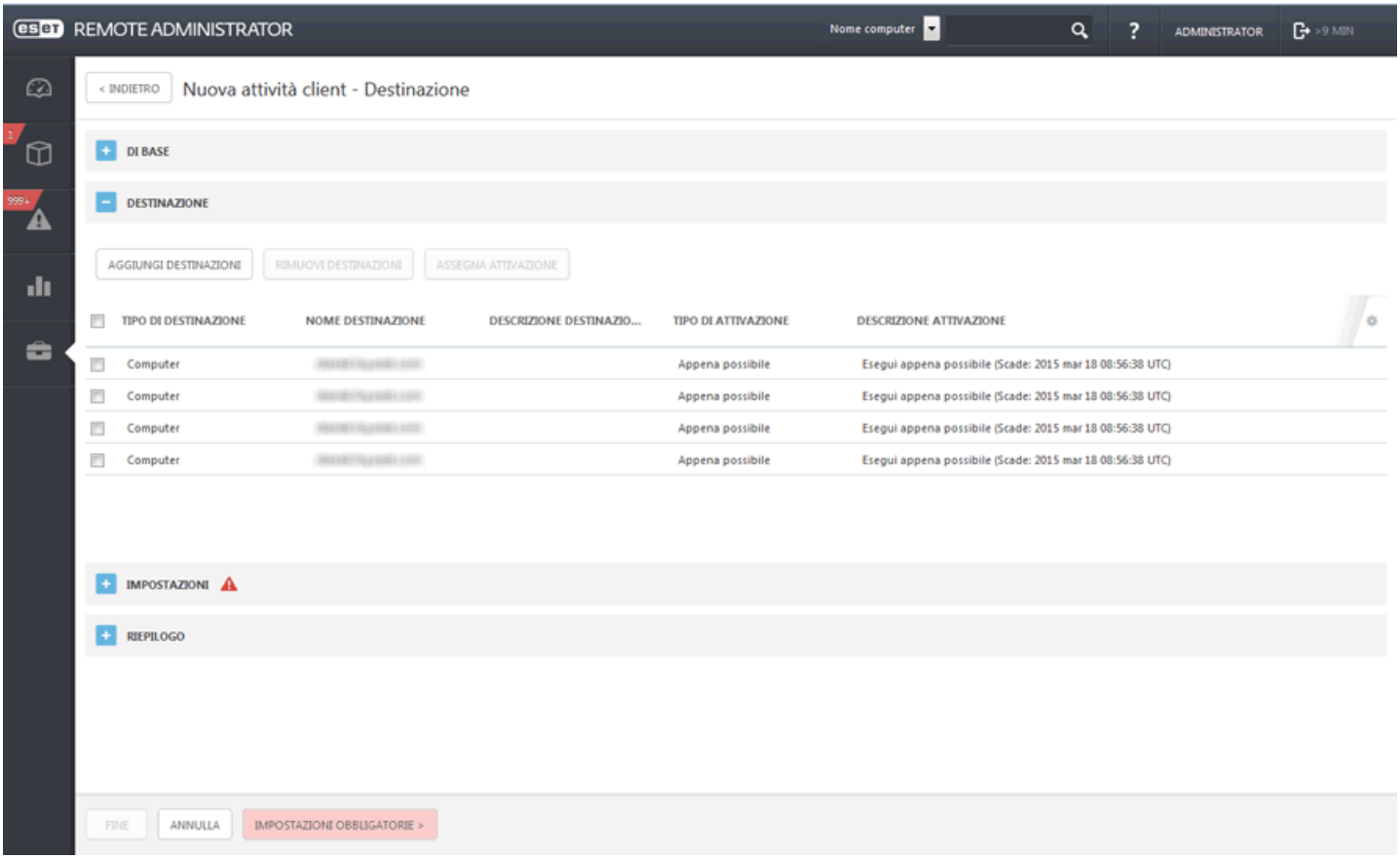
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.13 Carica file in quarantena

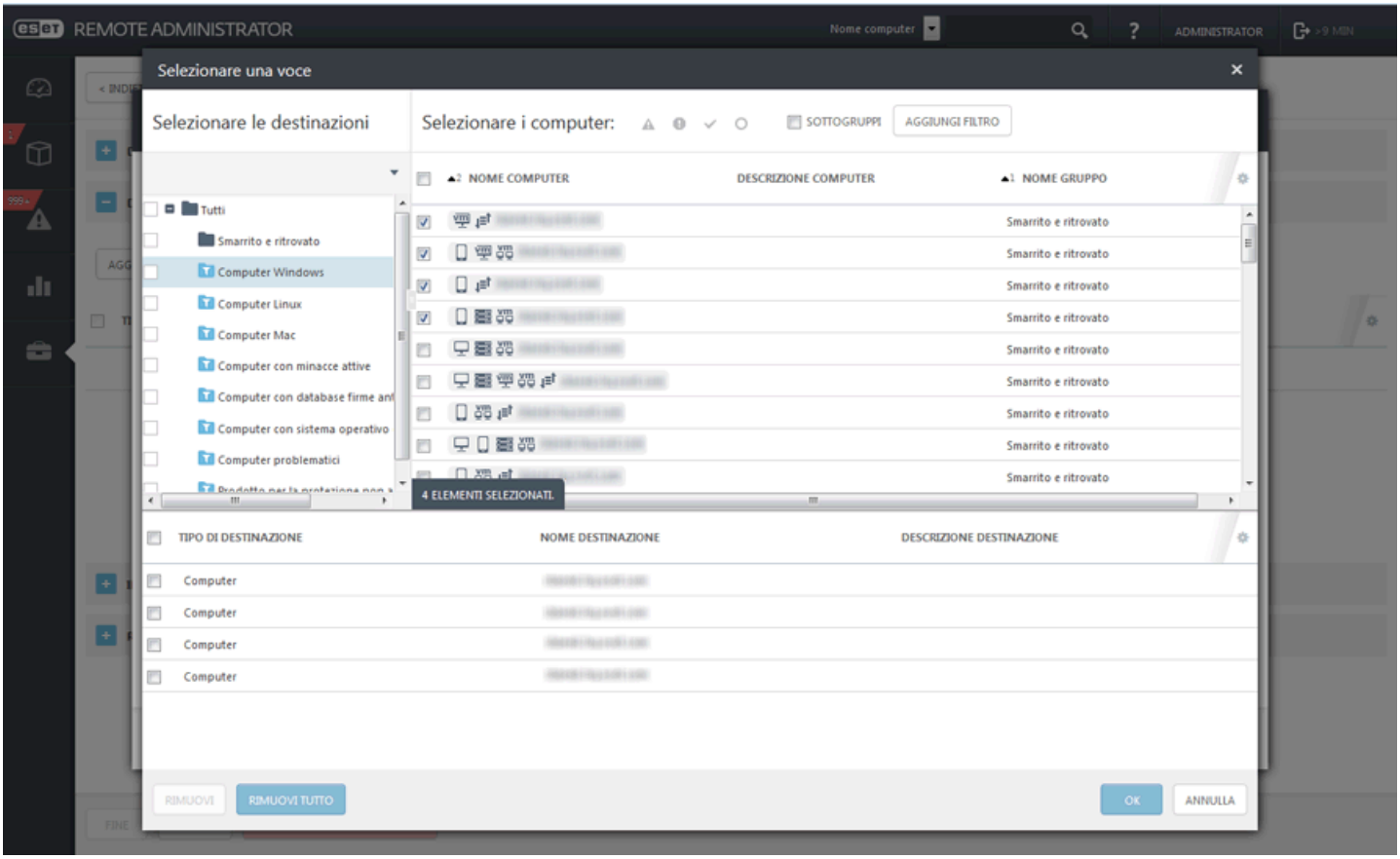
L'attività **Carica file in quarantena** viene utilizzata per gestire i file messi in quarantena sui client.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Oggetto in quarantena**: selezionare un oggetto specifico dalla quarantena.
- **Password oggetto**: inserire una password per crittografare l'oggetto per motivi di sicurezza. Tenere presente che la password verrà visualizzata nel rapporto corrispondente.
- **Percorso di caricamento**: inserire un percorso verso una posizione in cui si desidera caricare l'oggetto.
- **Carica nome utente/password**: se la posizione richiede un'autenticazione (condivisione di rete, ecc.), è necessario inserire le credenziali di accesso.

Riepilogo

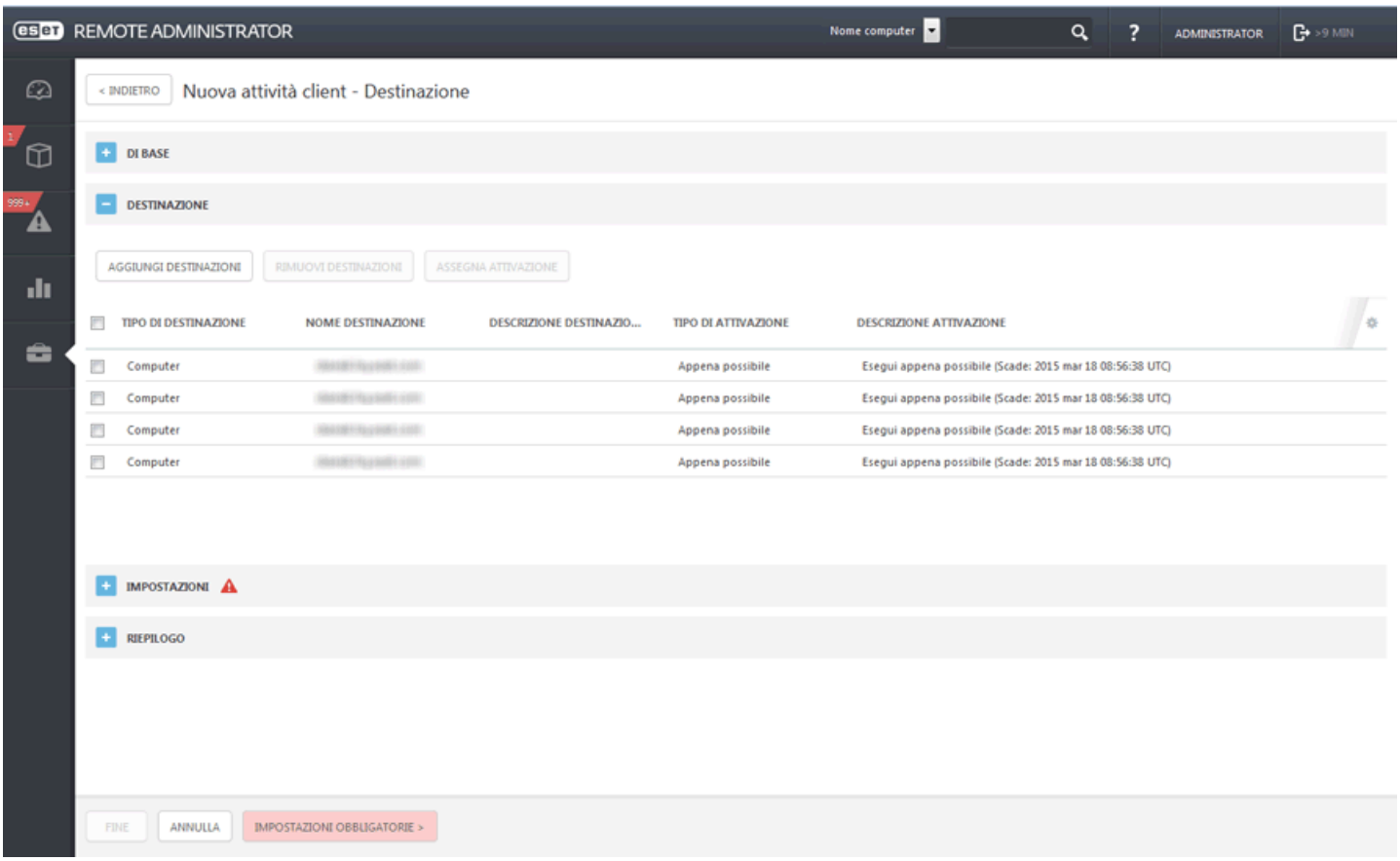
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.14 Aggiornamento database firme antivirali

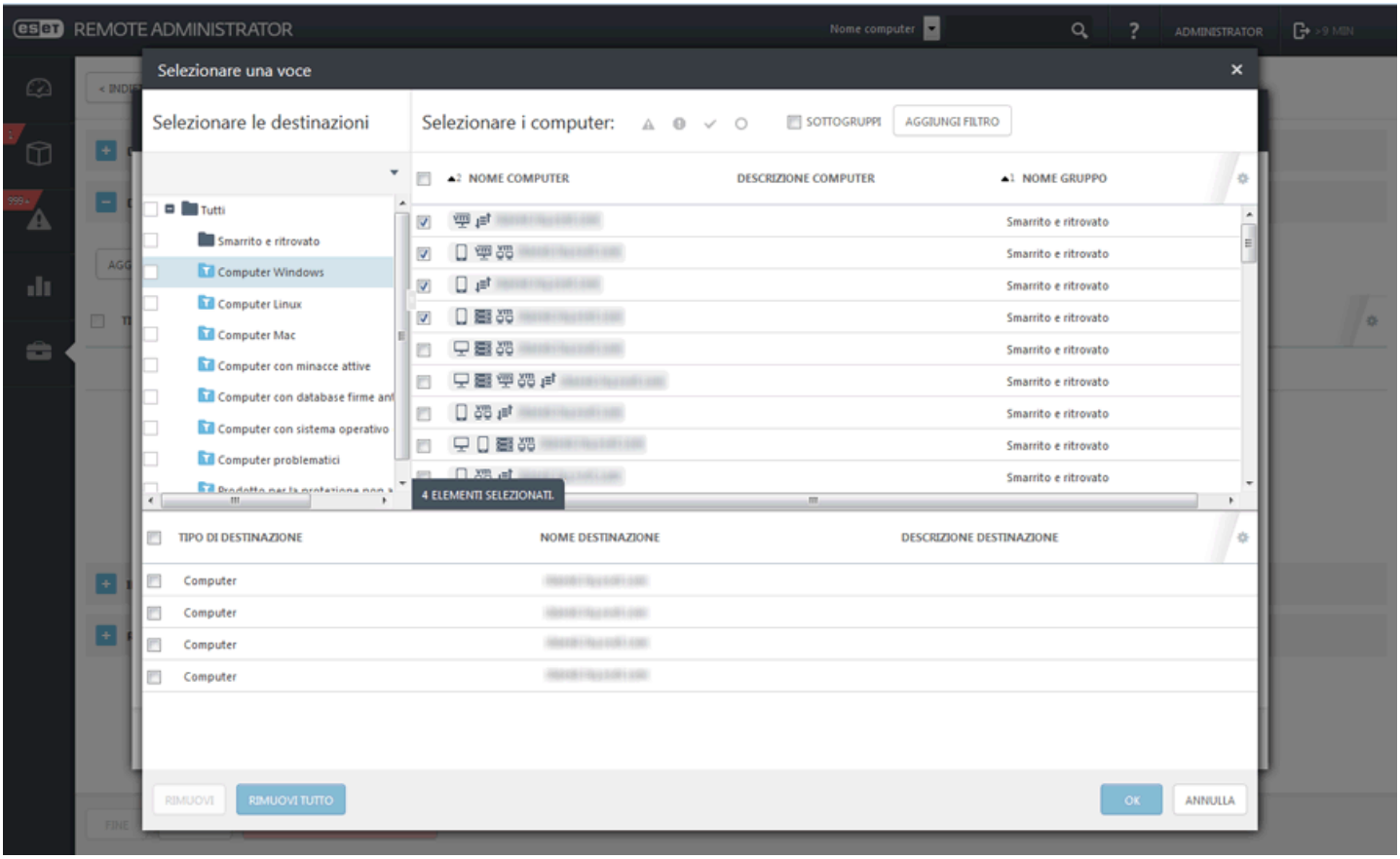
L'attività **Aggiornamento prodotto** forza l'aggiornamento del database delle firme antivirali del prodotto di protezione installato sui client. Si tratta di un'attività generica per tutti i prodotti installati sui sistemi.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Cancella cache aggiornamenti**: questa opzione, che elimina i file di aggiornamento temporanei dalla cache del client, viene utilizzata solitamente per riparare errori di aggiornamento del database delle firme antirivali.

Riepilogo

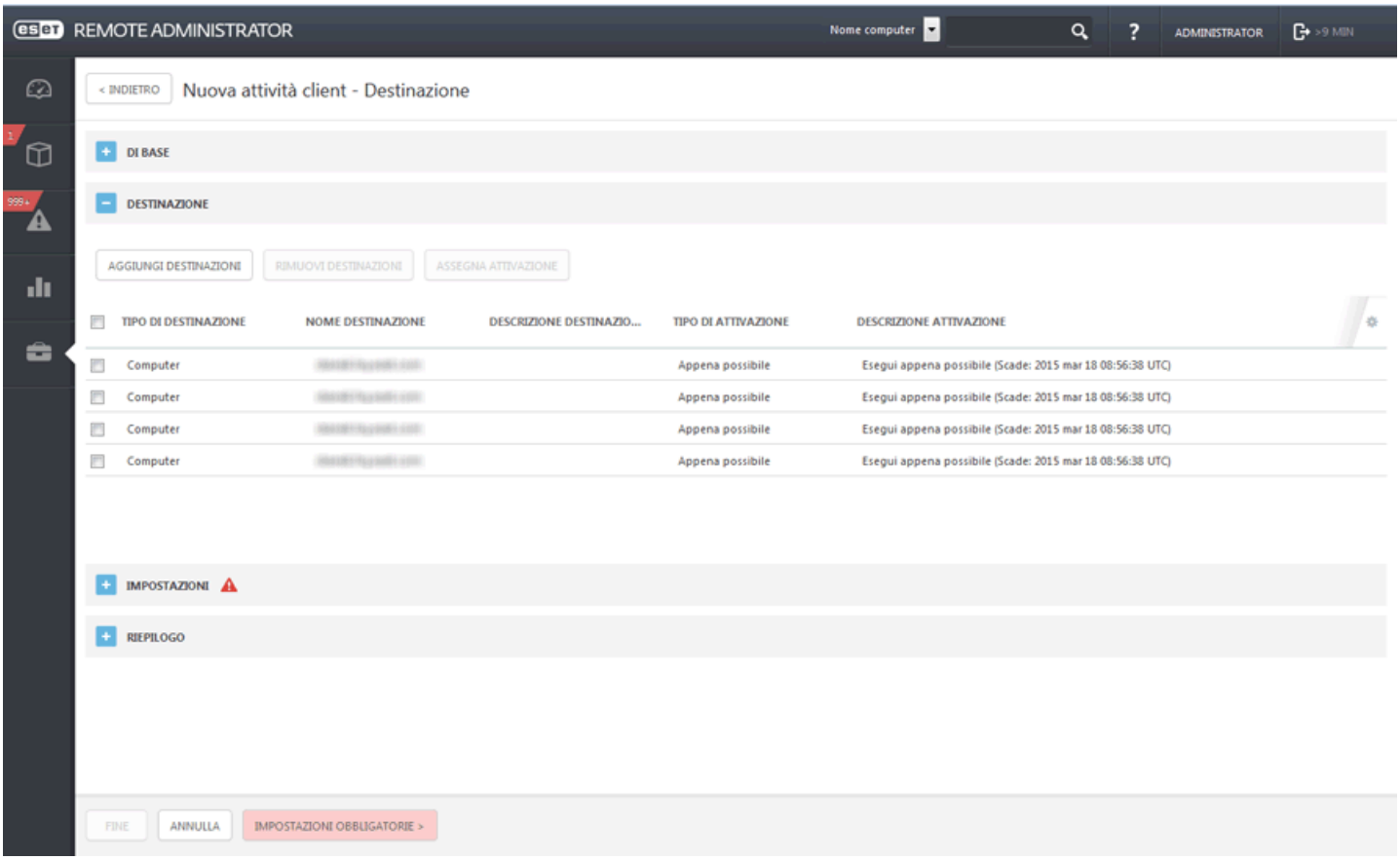
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.15 Rollback aggiornamento database firme antivirali

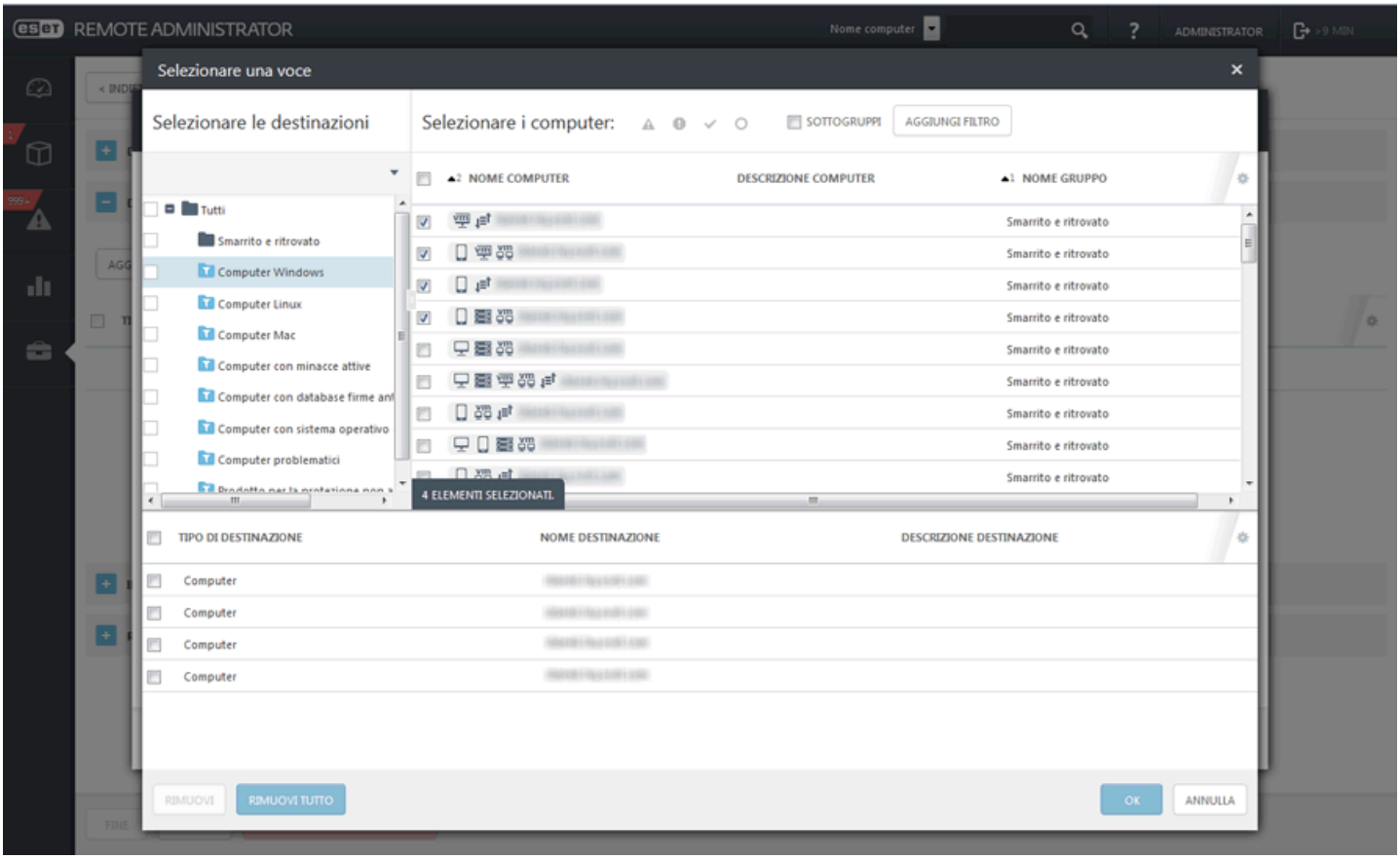
A volte un aggiornamento del database delle firme antivirali causa problemi oppure l'utente non desidera applicarlo a tutti i client (ad esempio, a scopo di testing o nel caso di aggiornamenti pre-rilascio). In questa circostanza, è possibile utilizzare l'attività **Rollback aggiornamento database firme antivirali**. In caso di utilizzo di questa attività, verrà ripristinata la versione precedente del database delle firme antivirali.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

Qui è possibile personalizzare le impostazioni del rollback dell'aggiornamento del database delle firme antivirali.

Azione

- **Aggiornamenti attivati**: gli aggiornamenti sono attivati e il client riceverà il successivo aggiornamento del database delle firme antivirali.
- **Rollback e disattiva aggiornamenti per il successivo**: gli aggiornamenti vengono disattivati per il periodo di tempo specifico nel menu a discesa **Disattiva intervallo** (24/36/48 ore o fino a revoca). Utilizzare l'opzione Fino a revoca con prudenza, in quanto rappresenta un potenziale rischio per la protezione.

Riepilogo

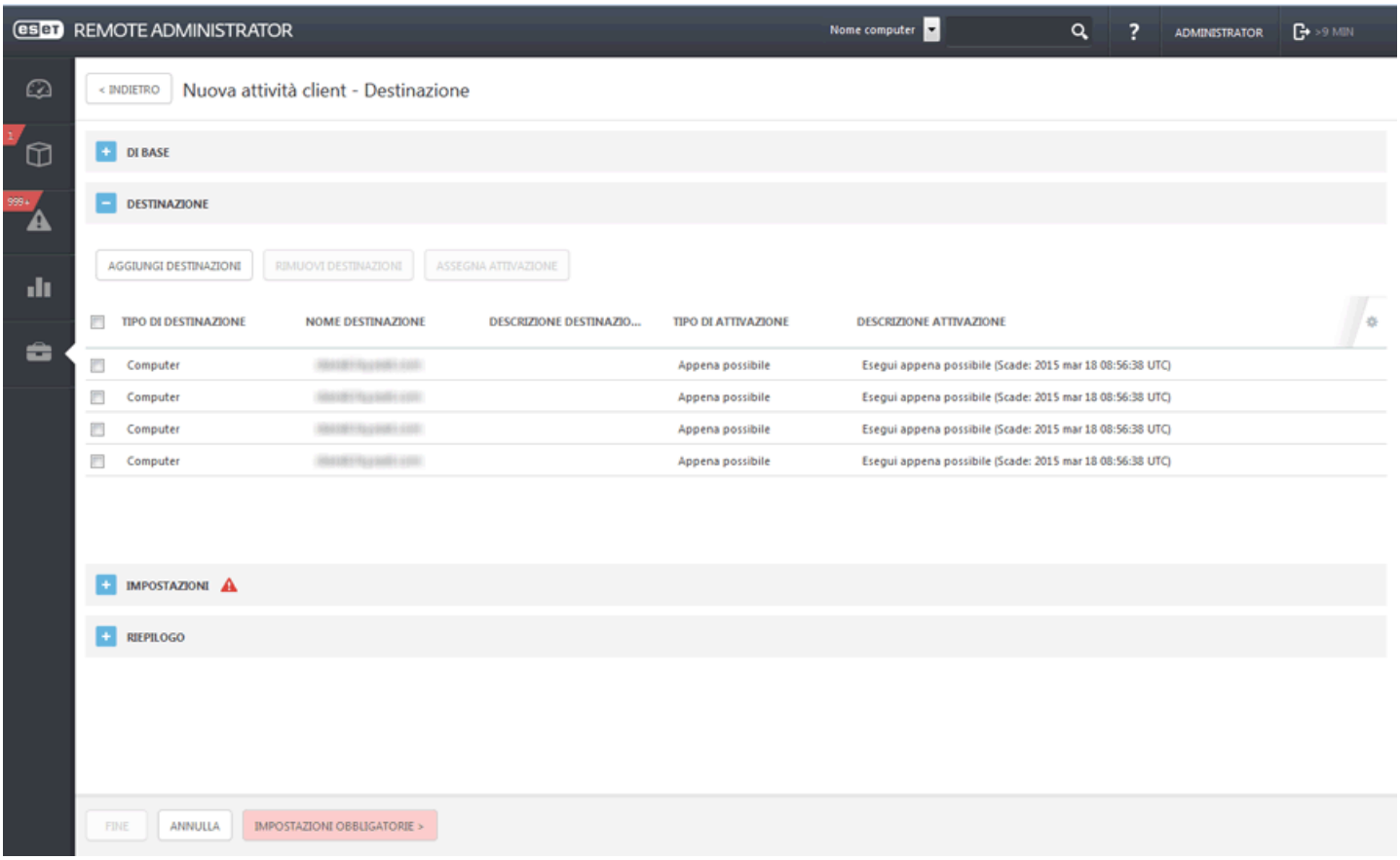
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.16 Visualizza messaggio

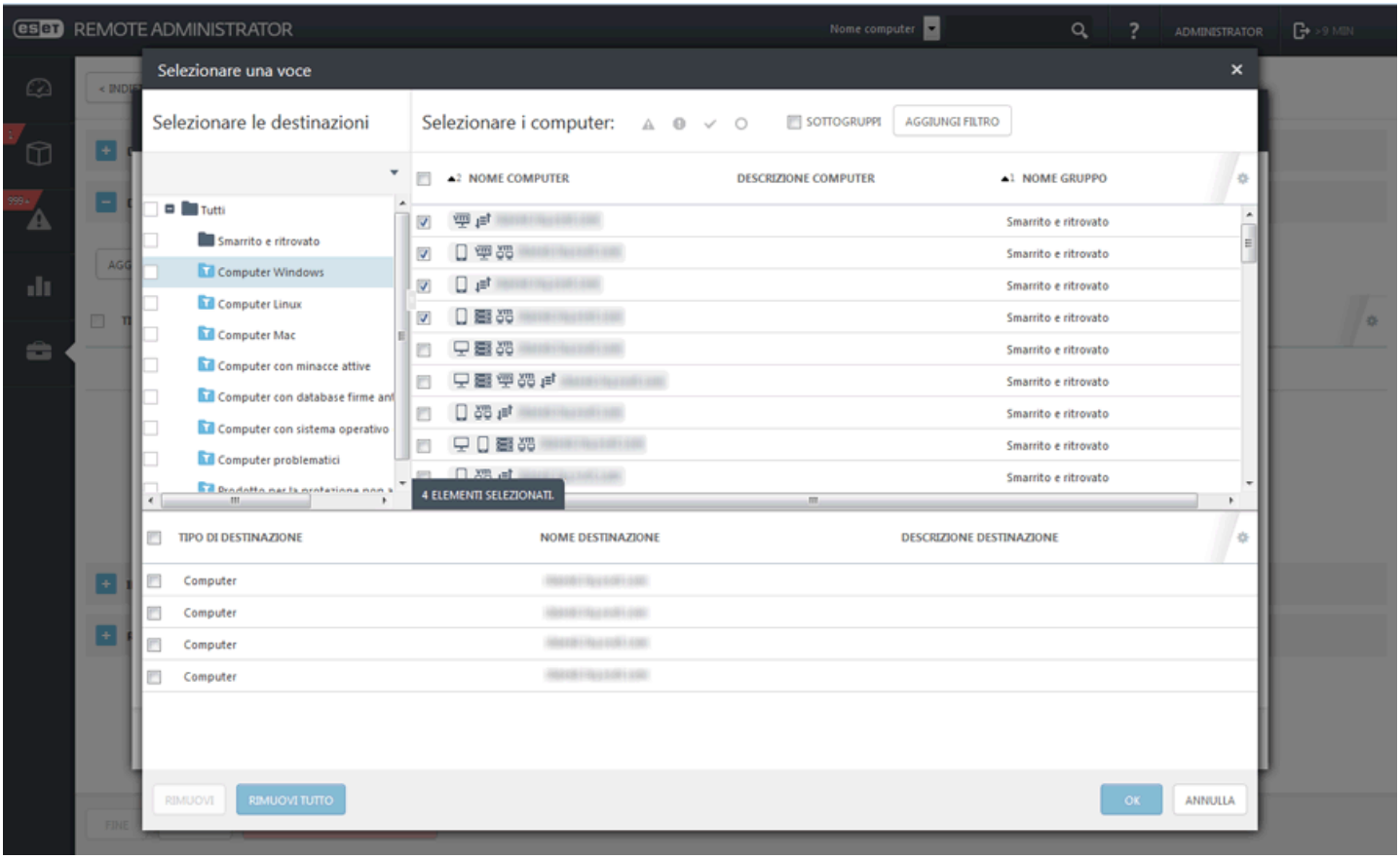
Questa funzionalità consente di inviare un messaggio a qualsiasi dispositivo (computer client, tablet, mobile, ecc.). Il messaggio sarà visualizzato sullo schermo per informare l'utente.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

È possibile immettere un **Titolo** e digitare il **Messaggio**.

Riepilogo

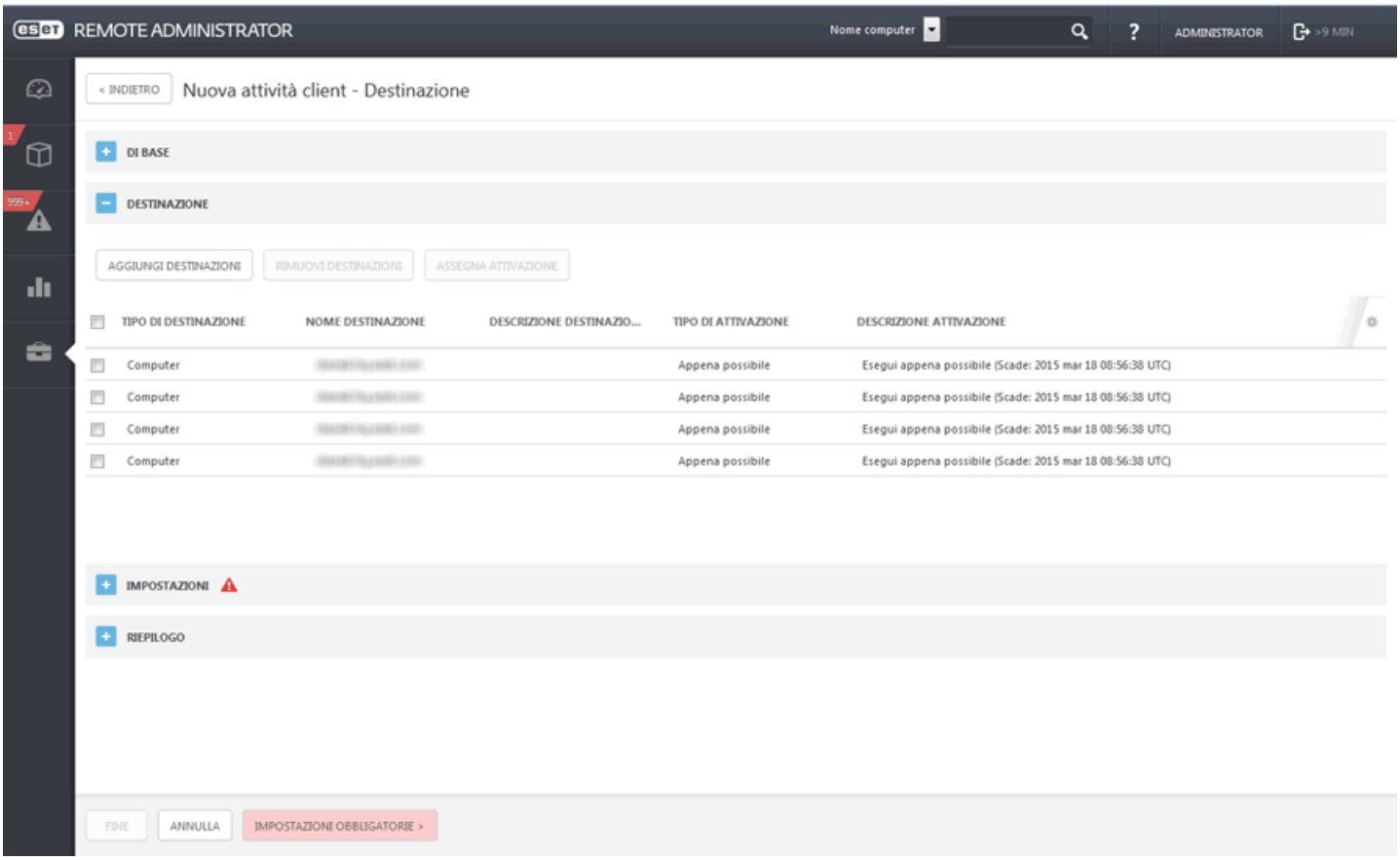
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.17 Azioni Anti-Furto

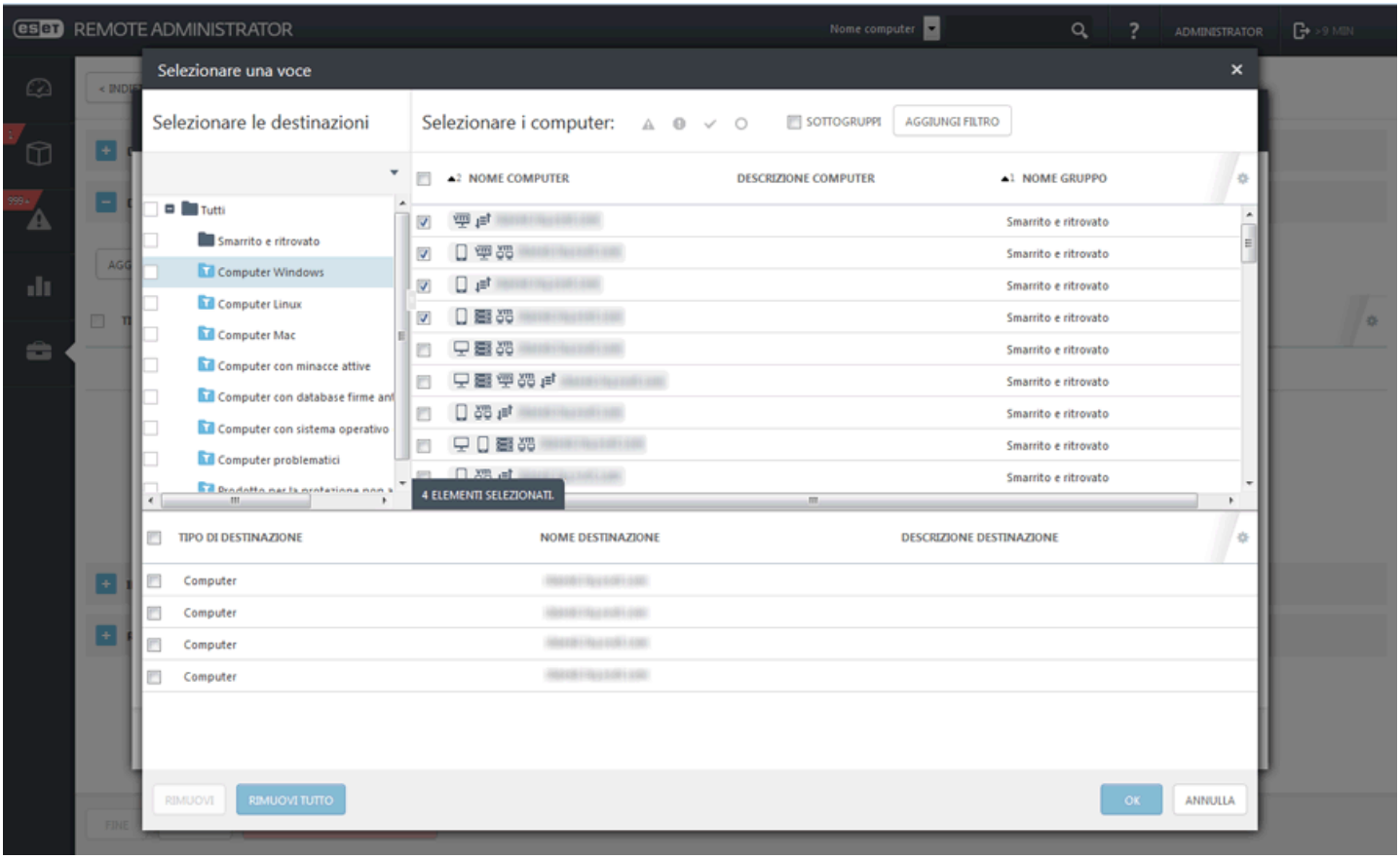
La funzione **Anti-Furto** protegge un dispositivo mobile dall'accesso non autorizzato. In caso di perdita o furto di un dispositivo mobile (registrato e gestito da ERA), alcune azioni vengono eseguite automaticamente, mentre altre possono essere eseguite tramite un'attività client. Se un utente non autorizzato sostituisce la Scheda SIM con una scheda SIM non attendibile, il dispositivo verrà **bloccato** automaticamente da ESET Endpoint Security for Android e un SMS di avviso verrà inviato ai numeri di telefono impostati dall'utente. Il messaggio includerà il numero di telefono della scheda SIM attualmente in uso, il numero **IMSI** (International Mobile Subscriber Identity) e il numero **IMEI** (International Mobile Equipment Identity) del telefono. L'utente non autorizzato non sarà a conoscenza dell'invio di questo messaggio poiché verrà cancellato automaticamente dai thread di messaggistica del dispositivo. È inoltre possibile richiedere le coordinate **GPS** del dispositivo mobile perso o di cancellare da remoto tutti i dati archiviati sul dispositivo tramite un'attività client.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

- **Trova**: il dispositivo risponderà con un messaggio di testo contenente le rispettive coordinate GPS. Se dopo 10 minuti è disponibile una posizione più precisa, il dispositivo invierà nuovamente il messaggio.
- **Blocca**: il dispositivo verrà bloccato. Il dispositivo può essere sbloccato utilizzando la password amministratore o il comando di sblocco.
- **Sblocca:** il dispositivo verrà sbloccato e potrà essere nuovamente riutilizzato. La scheda SIM attualmente presente nel dispositivo sarà salvata come SIM attendibile.
- **Sirena:** il dispositivo verrà bloccato ed emetterà un suono molto acuto per 5 minuti (oppure finché non verrà sbloccato).
- **Cancella:** tutti i dati accessibili sul dispositivo verranno cancellati (i file verranno sovrascritti). ESET Endpoint Security rimarrà installato sul dispositivo. L'operazione potrebbe richiedere alcune ore.
- **Ripristino avanzato impostazioni predefinite**: tutti i dati accessibili sul dispositivo verranno cancellati (le intestazioni dei file verranno distrutte) e sul dispositivo verranno ripristinate le impostazioni predefinite. L''operazione potrebbe richiedere alcuni minuti.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.2.18 Registrazione dispositivo

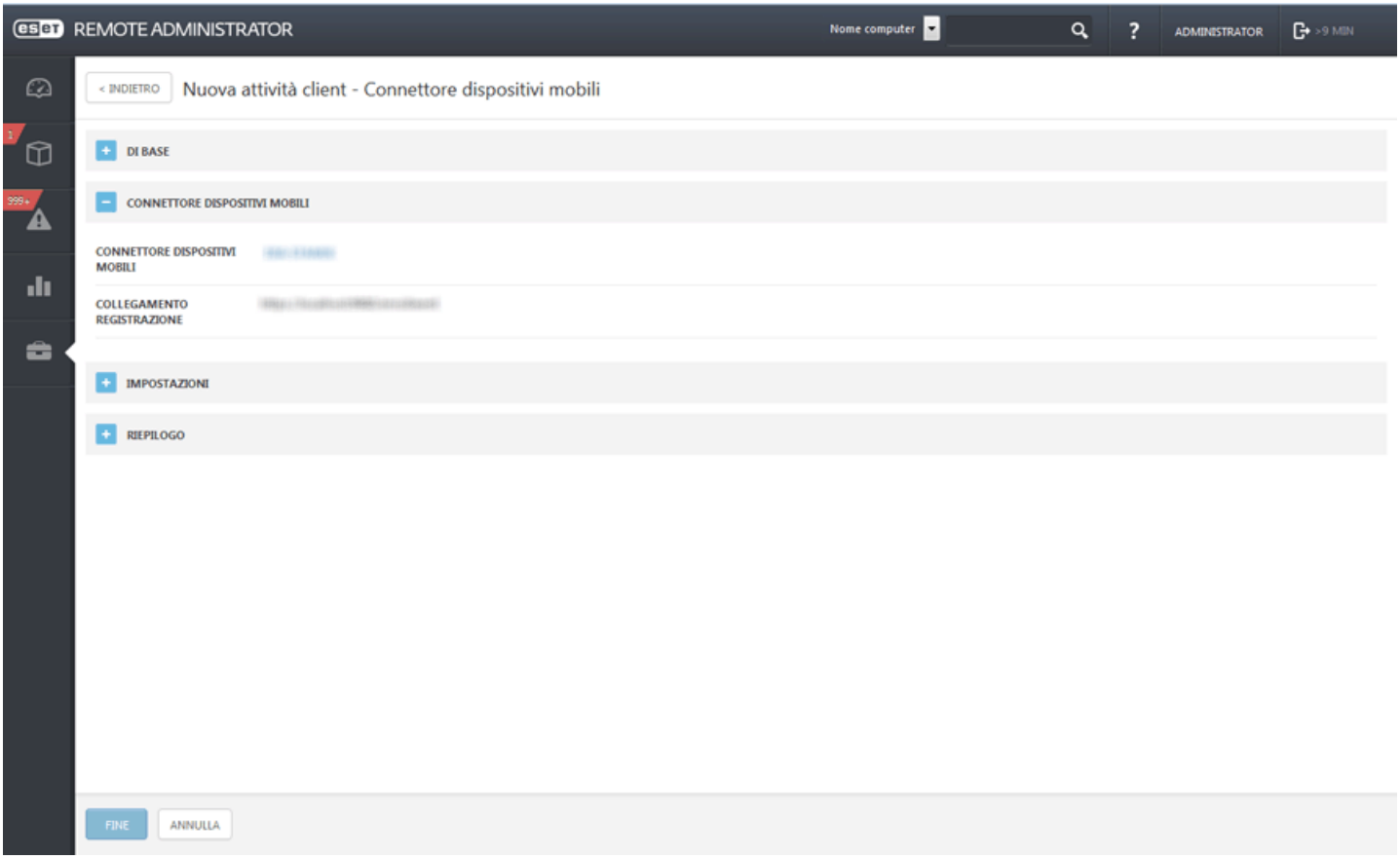
I telefoni cellulari possono essere gestiti dal server ERA tramite l'app mobile ESET Endpoint Security for Android versione 2. Per iniziare a gestire i dispositivi mobili è necessario registrarli in ERA. La Registrazione dispositivo viene eseguita tramite un'Attività client.

Di base

Immettere un **Nome** e una **Descrizione** (facoltativa).

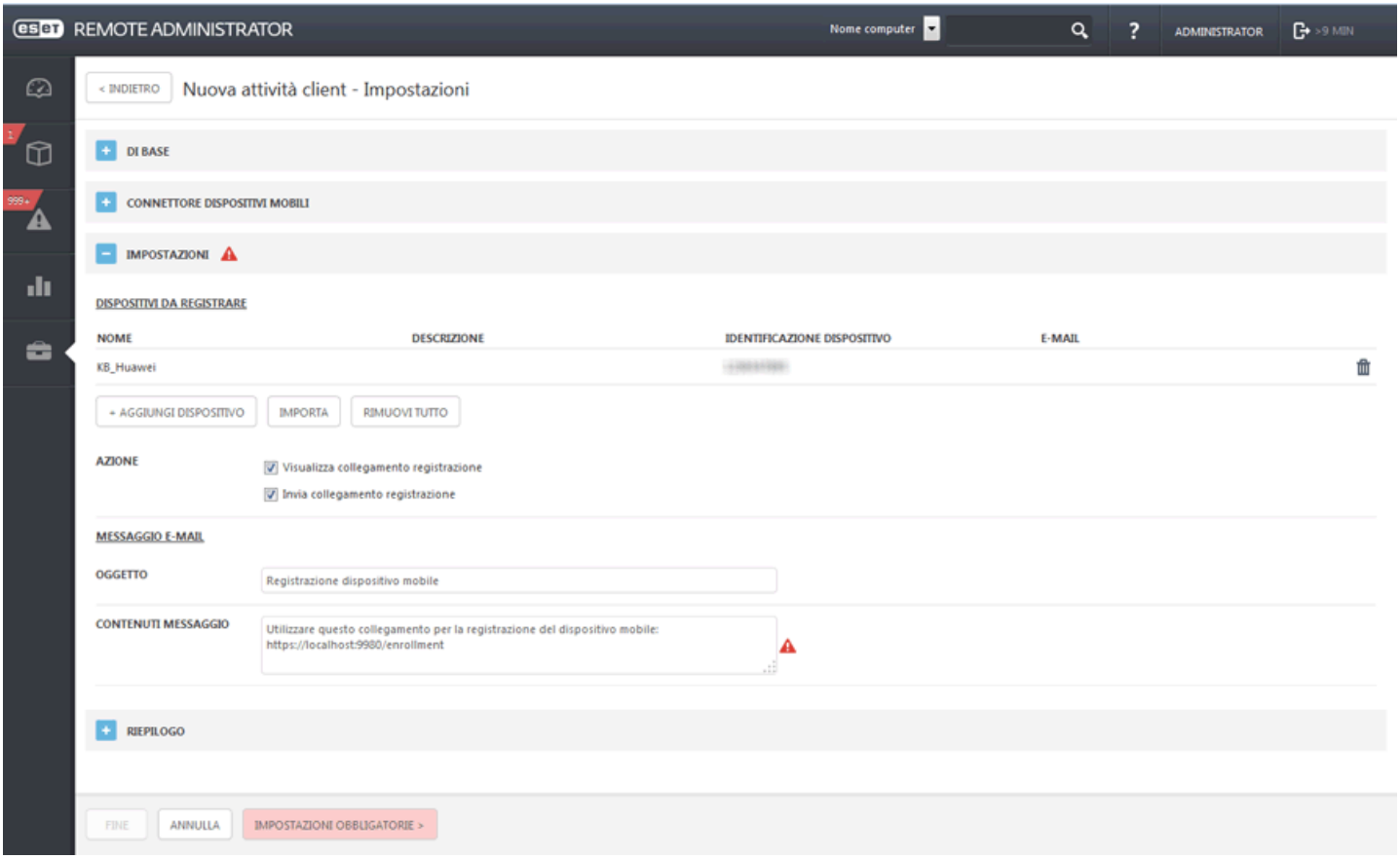
Connettore dispositivi mobili

Selezionare la macchina dove è installato il Connettore dispositivi mobili. Verrà visualizzato automaticamente un collegamento per la registrazione (URL). Se dopo aver fatto clic su Seleziona non viene visualizzato alcun collegamento, verificare che il server del Connettore dispositivi mobili sia accessibile. Se il Connettore dispositivi mobili ancora non è installato, consultare i capitoli Installazione di Connettore dispositivi mobili: Windows o Linux di questa guida per le istruzioni di installazione.



Impostazioni

Immettere il **Nome** del dispositivo mobile (che sarà visualizzato nell'elenco di Computer) e una **Descrizione** (facoltativa). Immettere il numero IMEI del dispositivo mobile specifico che si desidera aggiungere. Si consiglia di immettere l'indirizzo **E-mail** associato al dispositivo mobile (il collegamento per la registrazione verrà infatti inviato a tale indirizzo e-mail). Fare clic su **+ Aggiungi dispositivo** per aggiungere un altro dispositivo mobile. È possibile aggiungere contemporaneamente più dispositivi. Specificare un'**Azione** selezionando la casella di controllo accanto a **Visualizza collegamento registrazione** e/o **Invia collegamento registrazione** (l'URL verrà inviato agli indirizzi e-mail associati al dispositivo). Se si desidera inviare un collegamento per la registrazione (opzione consigliata) al dispositivo mobile, è possibile modificare l'**Oggetto** e i **Contenuti messaggio**, ma fare attenzione a non modificare l'URL di registrazione.



Riepilogo

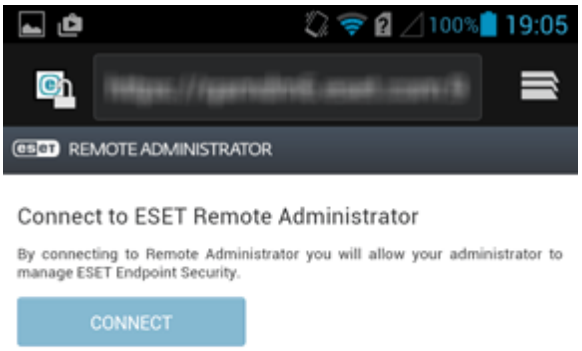
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

Fare clic su **Fine**: verrà visualizzato il collegamento per la registrazione (URL). Se non si specifica un indirizzo e-mail e se non è stata selezionata l'opzione **Invia collegamento registrazione**, è necessario immettere manualmente l'URL nel browser Web sul dispositivo mobile o inviarlo al dispositivo mobile tramite altri mezzi.

Quando ESET Endpoint Security for Android (EESA) è attivato sul dispositivo mobile, sono disponibili due scenari per la registrazione. Attivare EESA sul dispositivo mobile utilizzando l'attività del client Attivazione del prodotto ERA (scelta consigliata). L'altro scenario riguarda i dispositivi mobili sui quali l'applicazione EESA è già attivata.

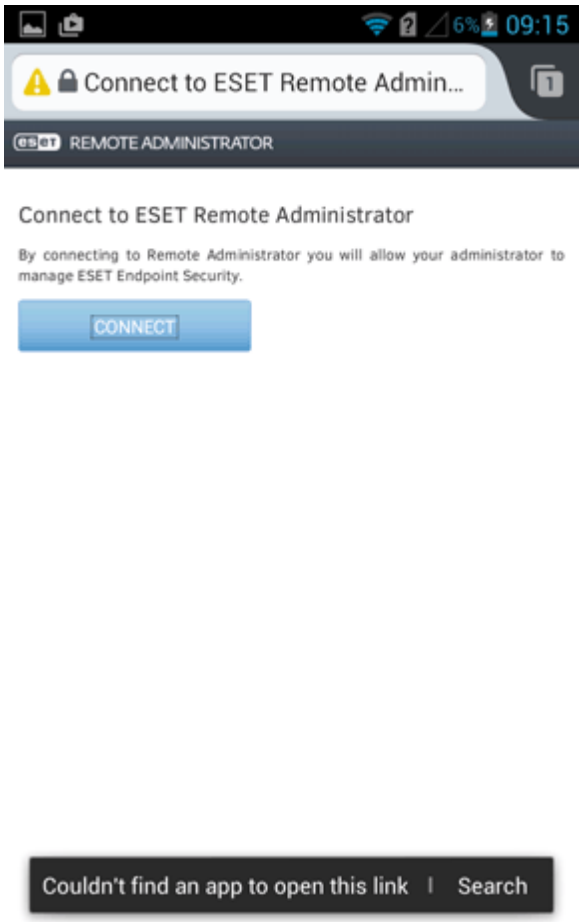
EESA non ancora attivato: attenersi ai passaggi illustrati di seguito per attivare il prodotto e registrare il dispositivo:

1. Toccare l'URL del collegamento per la registrazione ricevuto tramite e-mail oppure digitarlo manualmente nel browser, compreso il numero di porta (ad esempio, https://eramdm:9980). È probabile che venga richiesto di accettare un certificato SSL. Fare clic su Accetta se d'accordo, quindi su **Connetti**.

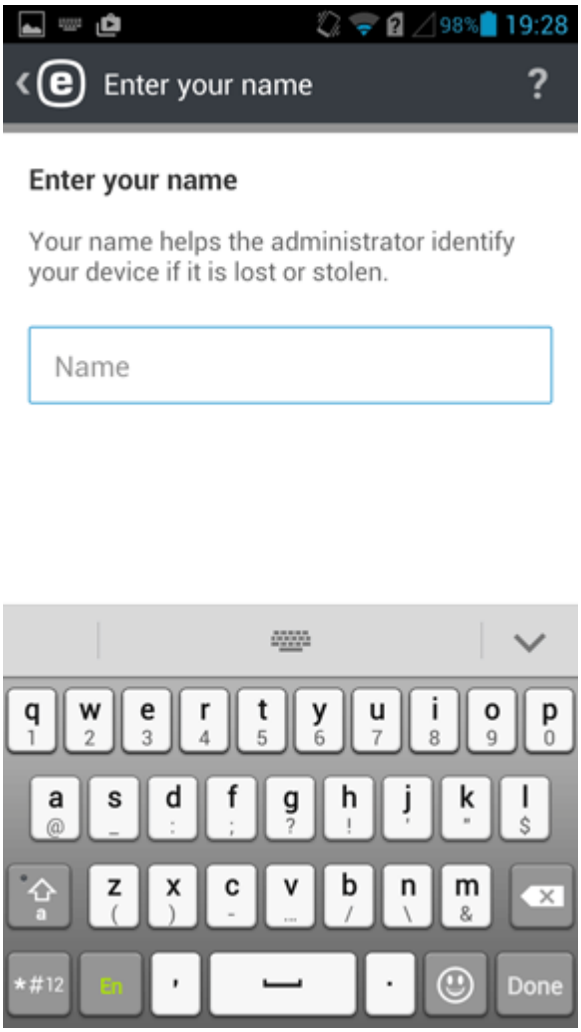

100% 19:05
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT

2. Se sul dispositivo mobile non è installato ESET Endpoint Security, l'utente verrà reindirizzato automaticamente allo store Google Play dove potrà scaricare l'applicazione.

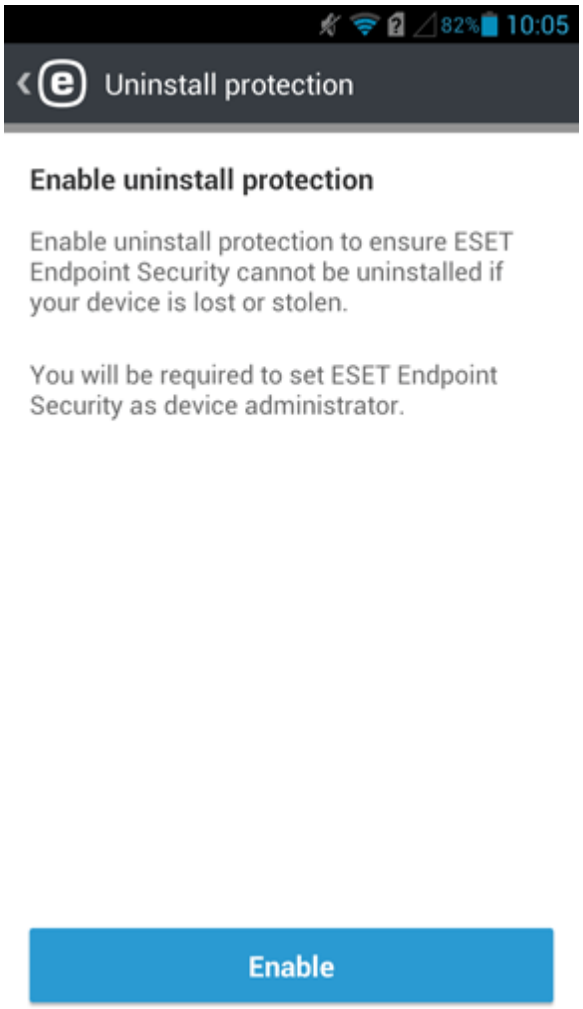
NOTA: se si riceve la notifica **Impossibile trovare l'app per aprire questo collegamento**, provare ad aprire il collegamento per la registrazione nel browser Web Android predefinito.


09:15
Connect to ESET Remote Admin...
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT
Couldn't find an app to open this link
Search

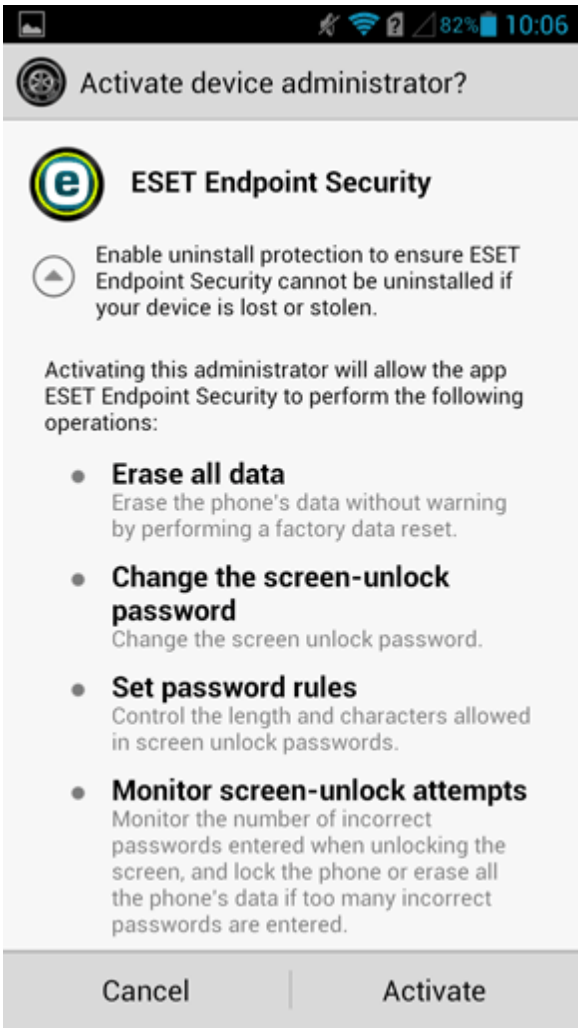
3. Immettere il nome dell'utente del dispositivo mobile.


98% 19:28
Enter your name
Enter your name
Your name helps the administrator identify your device if it is lost or stolen.
Name
Done

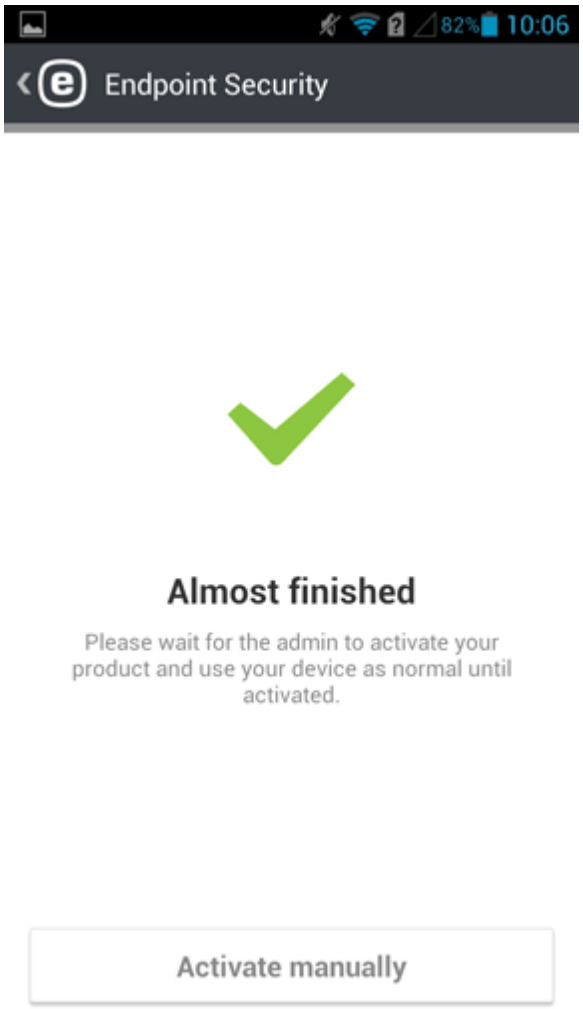
4. Toccare **Attiva** per consentire la disinstallazione della protezione.


82% 10:05
Uninstall protection
Enable uninstall protection
Enable uninstall protection to ensure ESET Endpoint Security cannot be uninstalled if your device is lost or stolen.
You will be required to set ESET Endpoint Security as device administrator.
Enable

5. Toccare **Attiva** per attivare l'amministratore del dispositivo.

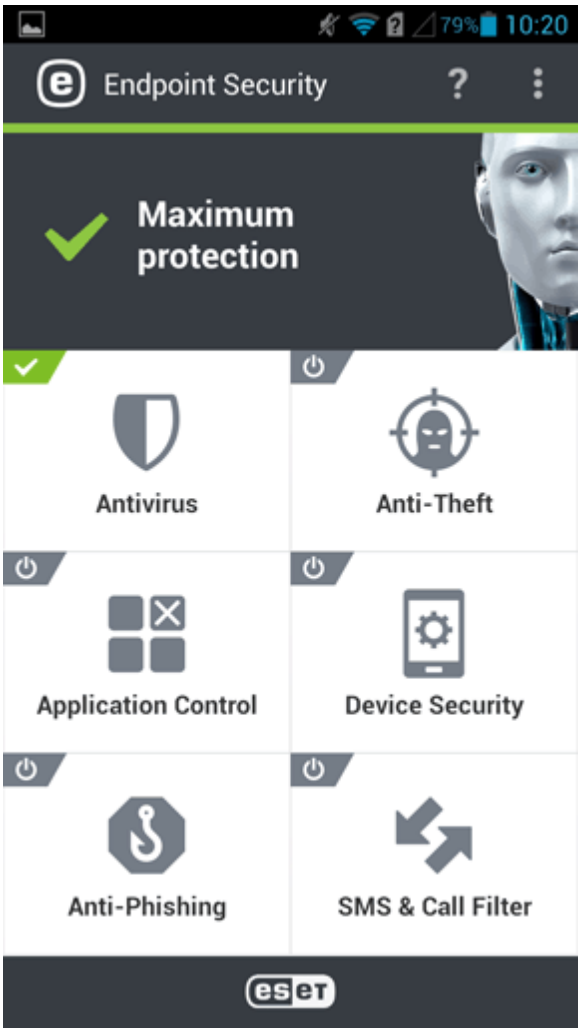

82% 10:06
Activate device administrator?
ESET Endpoint Security
Enable uninstall protection to ensure ESET Endpoint Security cannot be uninstalled if your device is lost or stolen.
Activating this administrator will allow the app ESET Endpoint Security to perform the following operations:
Erase all data
Erase the phone's data without warning by performing a factory data reset.
Change the screen-unlock password
Change the screen unlock password.
Set password rules
Control the length and characters allowed in screen unlock passwords.
Monitor screen-unlock attempts
Monitor the number of incorrect passwords entered when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are entered.
Cancel
Activate

6. A questo punto è possibile uscire dall'app EESA sul dispositivo mobile e aprire ERA Web Console.


82% 10:06
Endpoint Security
Almost finished
Please wait for the admin to activate your product and use your device as normal until activated.
Activate manually

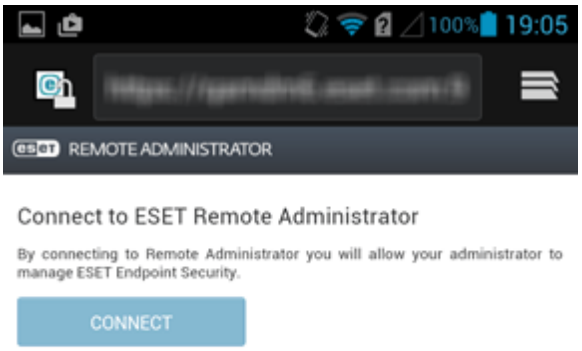
7. In ERA Web Console, accedere ad **Amministrazione** > **Attività client** > **Mobile** > Attivazione del prodotto e fare clic su **Nuovo**.
8. Selezionare il dispositivo mobile facendo clic su **Aggiungi destinazioni**.
9. In Impostazioni fare clic su <Scegliere licenza ESET> e selezionare la licenza appropriata. Fare clic su **Fine**.

Potrebbe essere necessario del tempo prima che l'attività del client Attivazione del prodotto sia eseguita sul dispositivo mobile. Al termine della corretta esecuzione dell'attività, l'app EESA è attivata e il dispositivo mobile è gestito da ERA. L'utente potrà ora utilizzare l'app EESA. All'apertura dell'app EESA, viene visualizzato il menu principale:



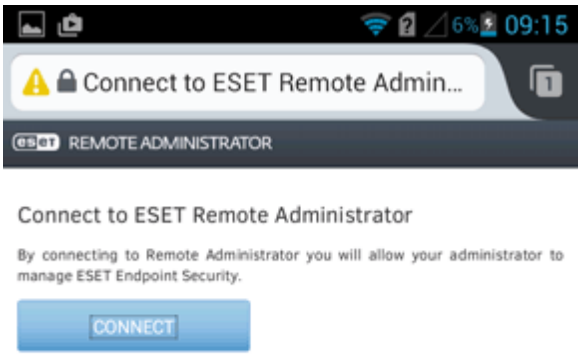
EESA già attivato: attenersi ai passaggi illustrati di seguito per registrare il dispositivo:

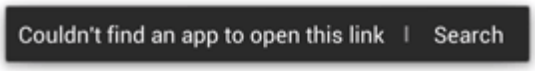
1. Toccare l'URL del collegamento per la registrazione ricevuto tramite e-mail oppure digitarlo manualmente nel browser, compreso il numero di porta (ad esempio, *https://eramdm:9980*). È probabile che venga richiesto di accettare un certificato SSL. Fare clic su Accetta se d'accordo, quindi su **Connetti**.


100% 19:05
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT

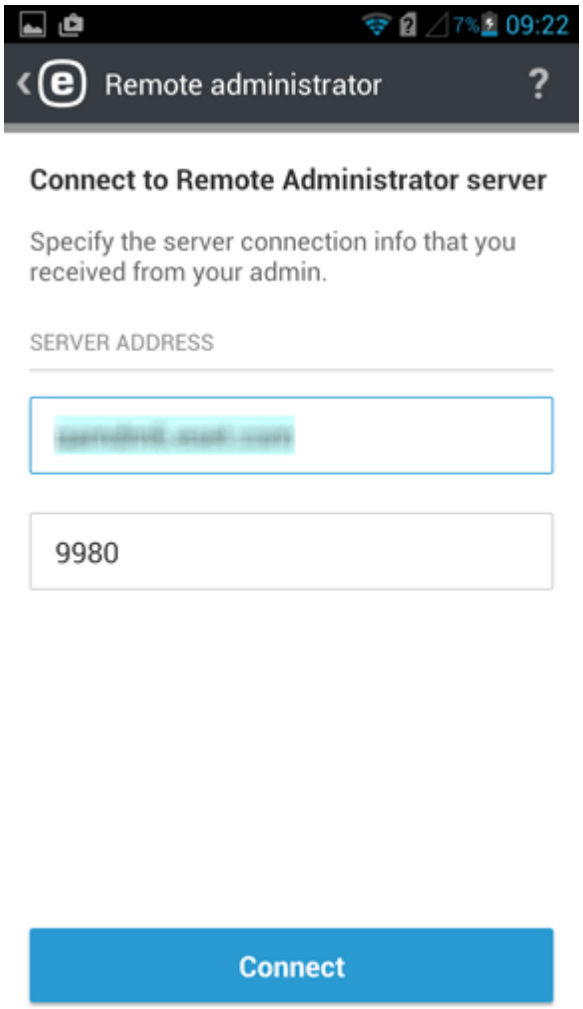
NOTA: se sul dispositivo mobile non è installato ESET Endpoint Security, l'utente verrà reindirizzato automaticamente allo store Google Play dove potrà scaricare l'applicazione.

NOTA: se si riceve la notifica **Impossibile trovare l'app per aprire questo collegamento**, provare ad aprire il collegamento per la registrazione nel browser Web Android predefinito.

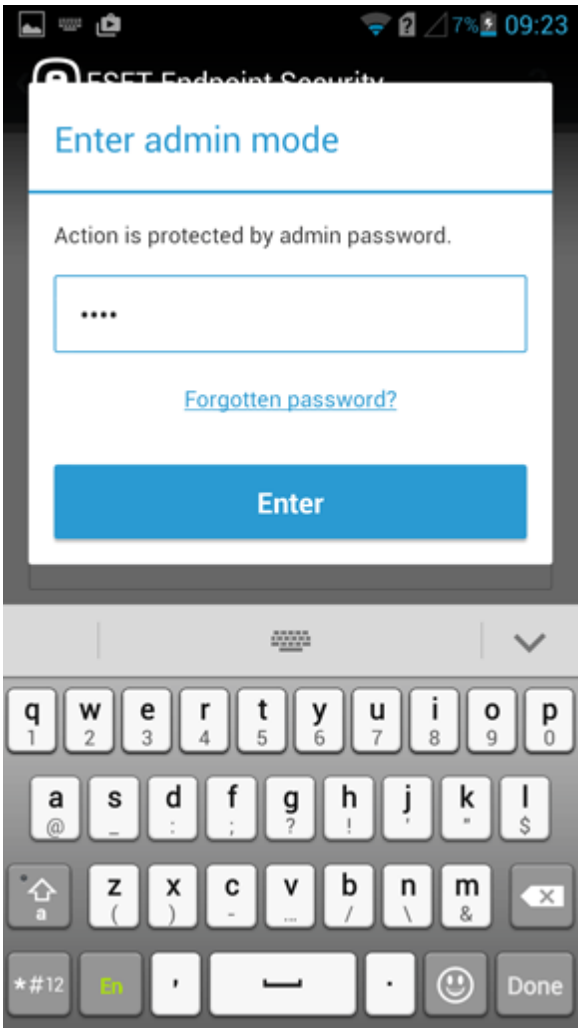

09:15
Connect to ESET Remote Admin...
REMOTE ADMINISTRATOR
Connect to ESET Remote Administrator
By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.
CONNECT



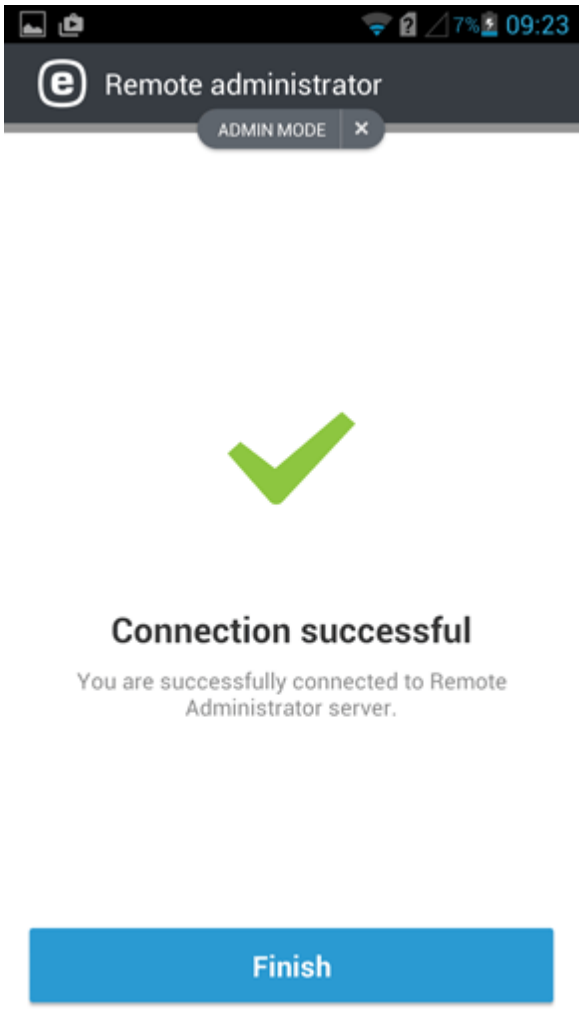
2. Verificare i dettagli della connessione (indirizzo e porta del server Connettore dispositivi mobili) e fare clic su **Connetti**.



3. Immettere la password della modalità amministratore di ESET Endpoint Security nel campo vuoto e toccare Invio.



4. Questo dispositivo è ora gestito da ERA. Toccare Fine.



6.1.3.2.19 Interrompi gestione (disinstallare agente ERA)

- **Desktop**: questa attività rimuoverà l'agente installato sulla macchina su cui è installato MDM.
- **Mobile**: questa attività consente di annullare la registrazione MDM dal dispositivo mobile.

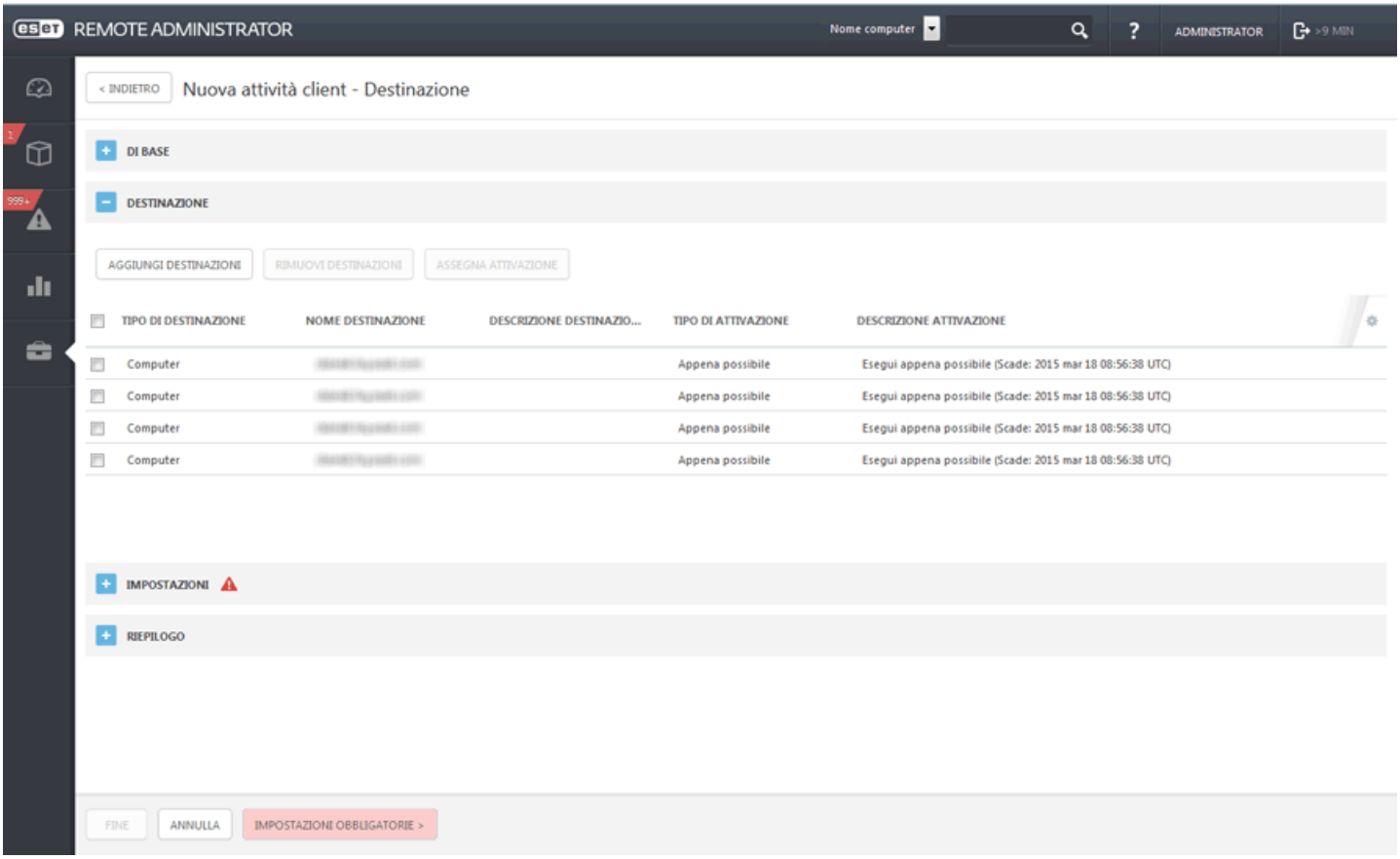
Se il dispositivo non è più gestito (l'agente è stato rimosso), nei prodotti gestiti potrebbero rimanere alcune impostazioni.
Si consiglia di reimpostare alcune impostazioni predefinite (ad esempio protezione con password) attraverso l'utilizzo di un criterio prima che il dispositivo venga rimosso dalla gestione. Inoltre, tutte le attività in esecuzione sull'agente verranno abbandonate. In base alla replica, lo stato **In esecuzione**, **Terminata** o **Non riuscita** dell'attività potrebbe non essere visualizzato in modo accurato in ERA Web Console.

1. Se non si desidera mantenere alcune impostazioni speciali nel dispositivo, utilizzare un criterio del dispositivo per ripristinare i valori predefiniti (o i valori desiderati).
2. Prima di eseguire questa operazione, è consigliabile attendere qualche minuto per essere certi che i criteri dal punto 1 abbiano terminato la replica sul computer di destinazione prima di cancellare il computer dall'elenco in ERA.
3. Prima di eseguire questa operazione, è consigliabile attendere qualche minuto per essere certi che i criteri dal punto 2 abbiano terminato la replica sul computer di destinazione.

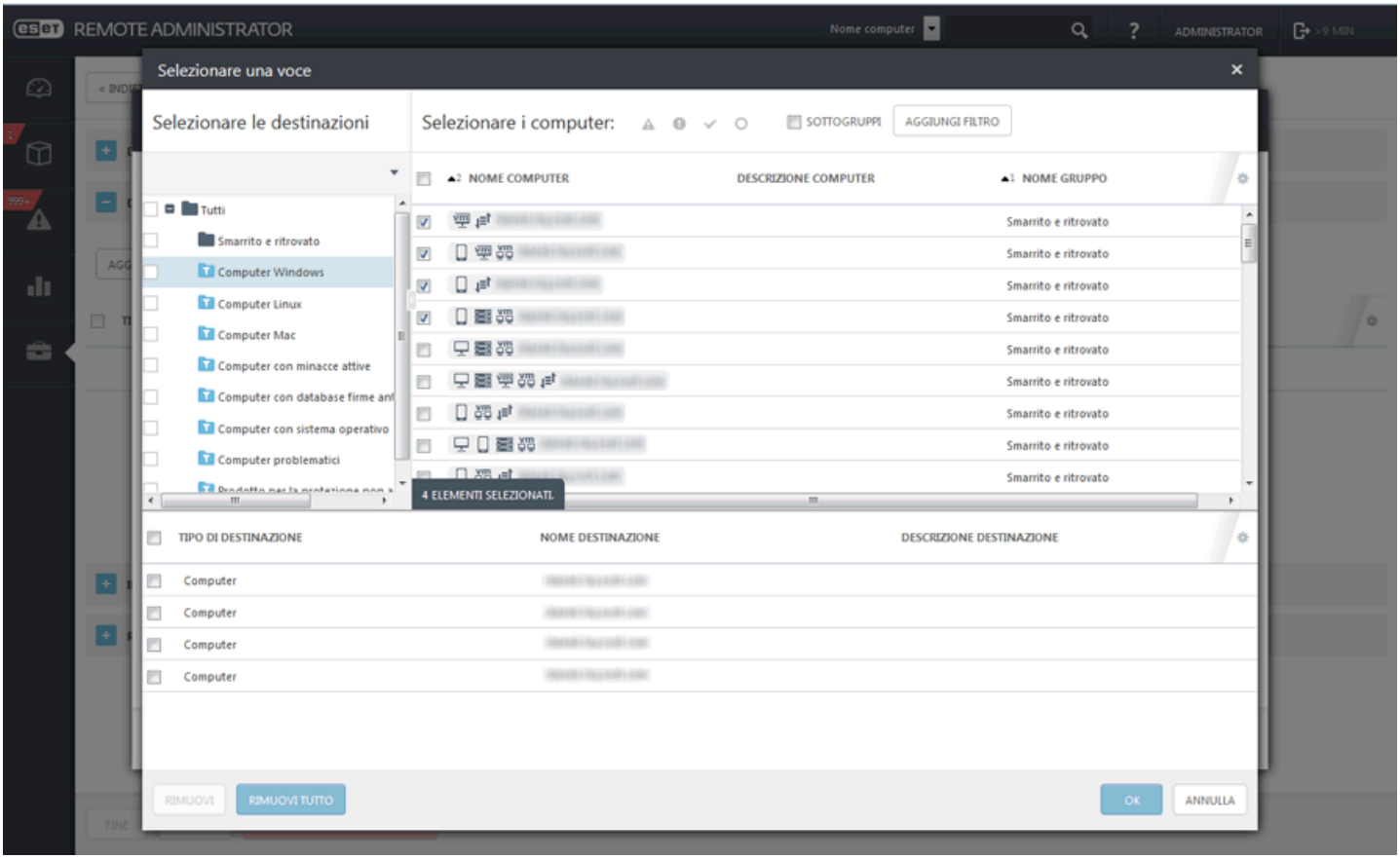
NOTA: non sono disponibili impostazioni per questa attività.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Riepilogo

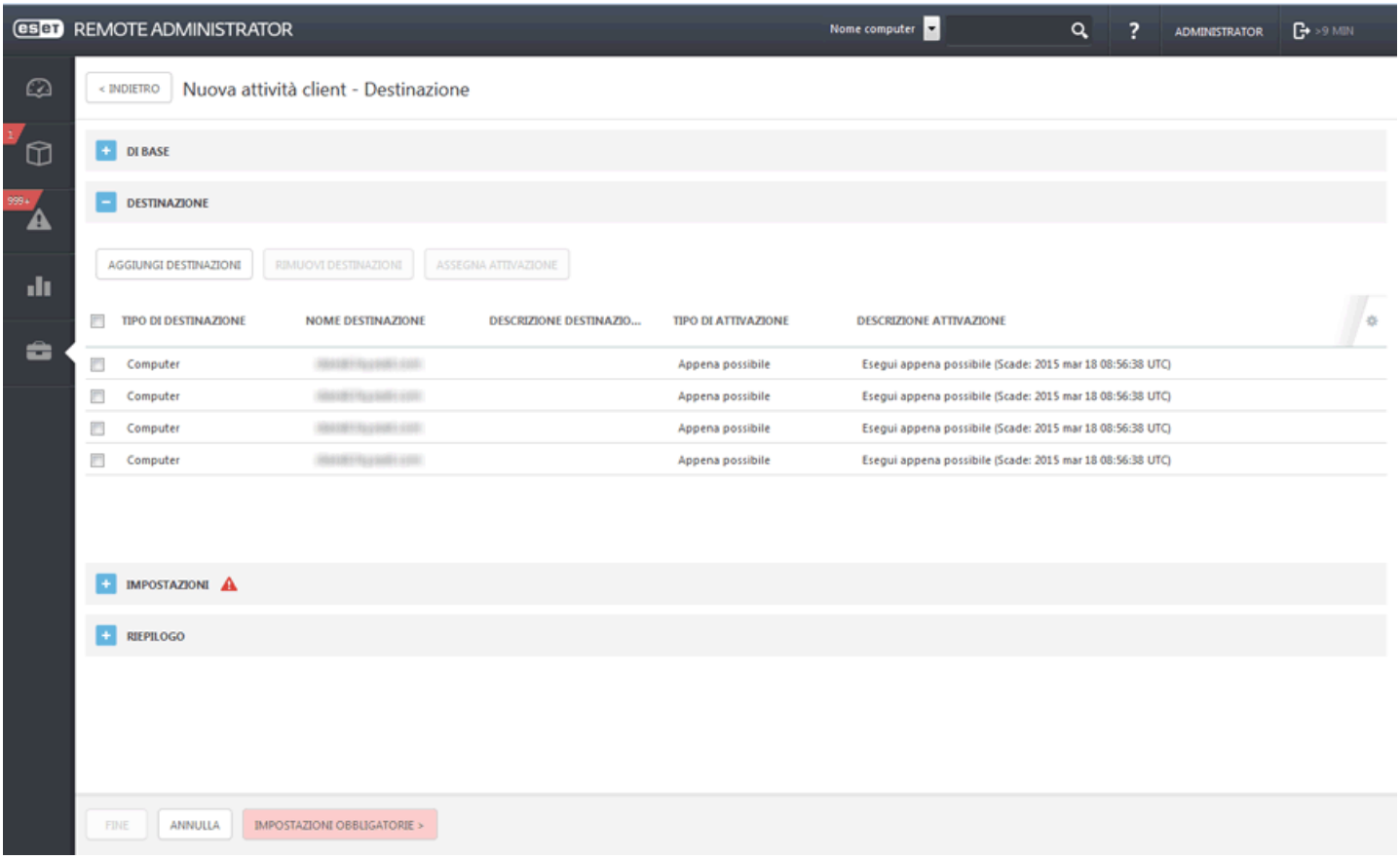
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.3 Esporta configurazione prodotti gestiti

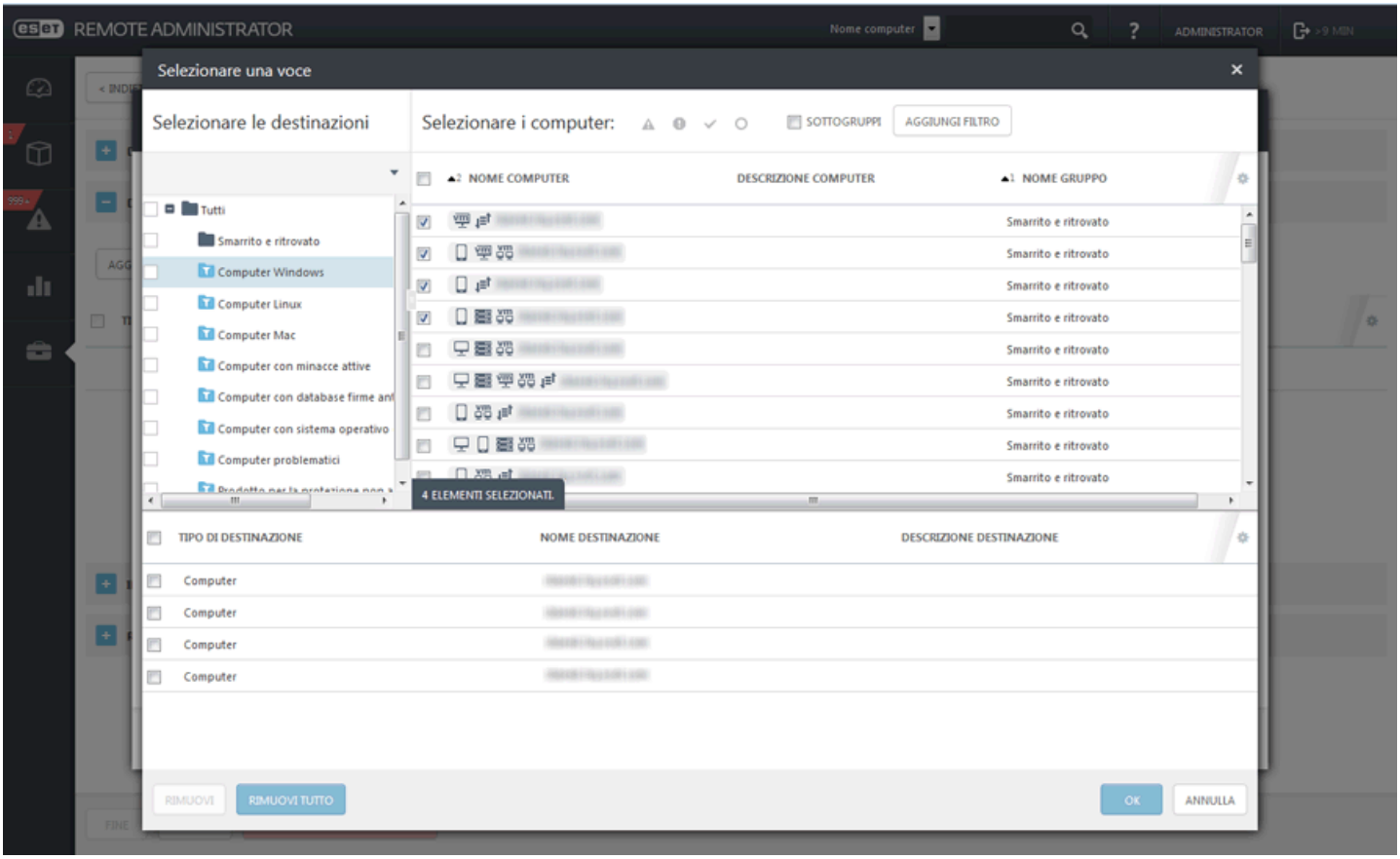
L'attività **Esporta configurazione prodotti gestiti** viene utilizzata per esportare le impostazioni di singoli componenti ERA o prodotti di protezione ESET installati su uno o più client.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Impostazioni

Esporta impostazioni configurazione prodotti gestiti

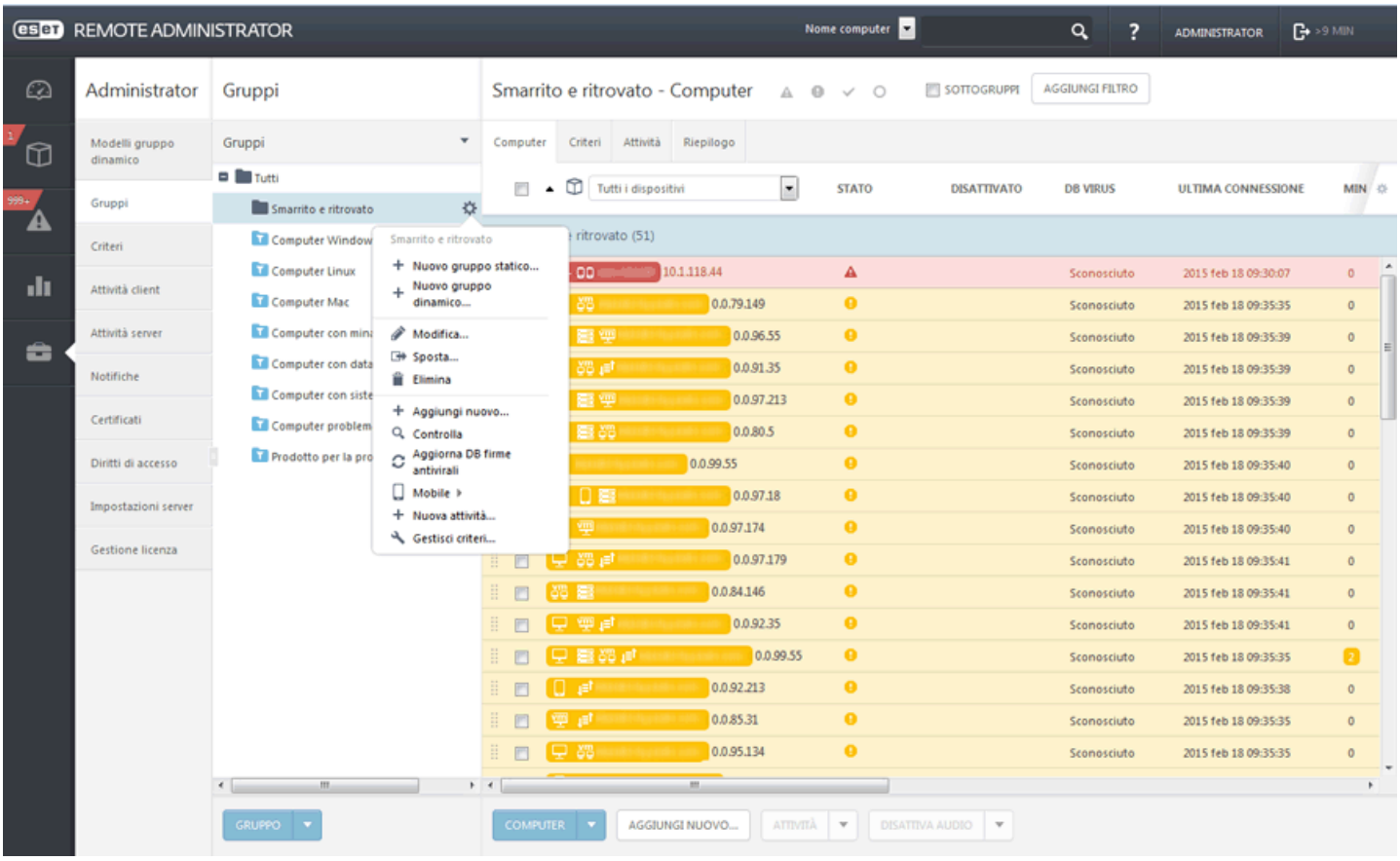
- **Prodotto**: selezionare un componente ERA o un prodotto di protezione client per il quale si desidera esportare la configurazione.

Riepilogo

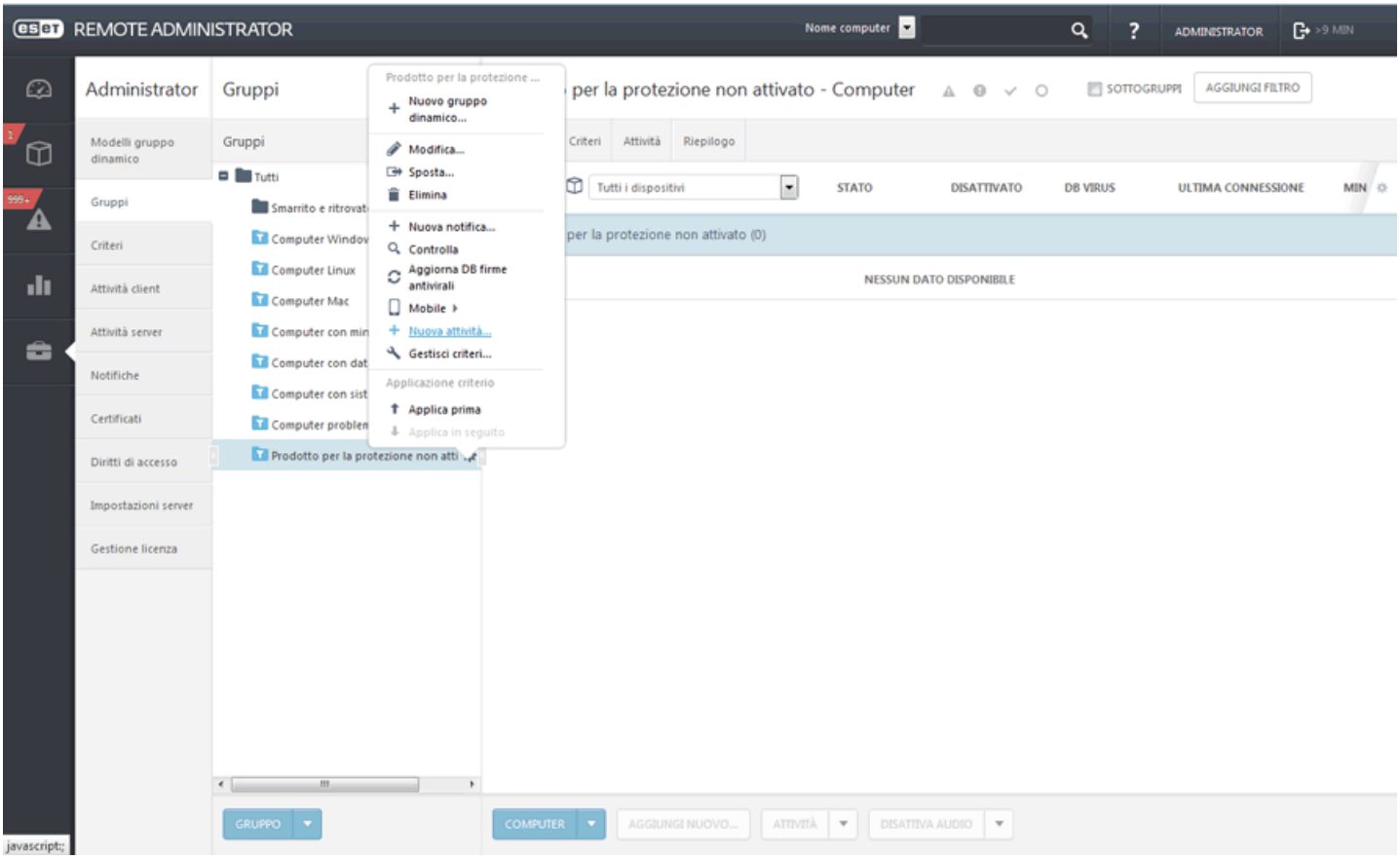
Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

6.1.3.4 Assegna attività a gruppo

Fare clic su **Amministrazione** > **Gruppi** > selezionare gruppo **Statico** o **Dinamico** > ⚙ accanto al gruppo selezionato, oppure fare clic su **Gruppo** > **+ Nuova attività**



La stessa procedura può essere eseguita da **Computer**, selezionare **Statico** o **Dinamico** e fare clic su ⚙ > **+ Nuova attività**

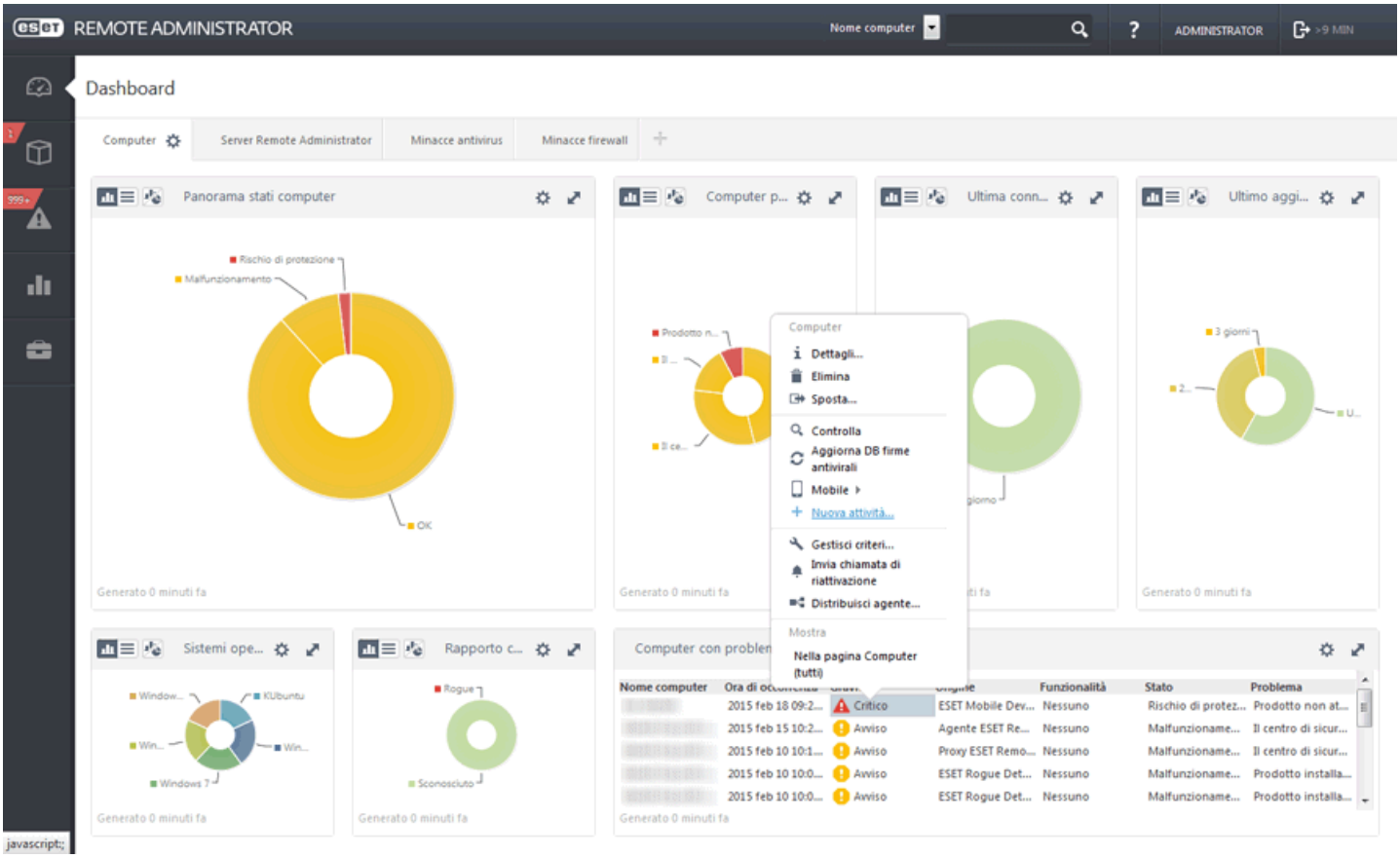


Verrà visualizzata una finestra della Procedura guidata nuova attività client.

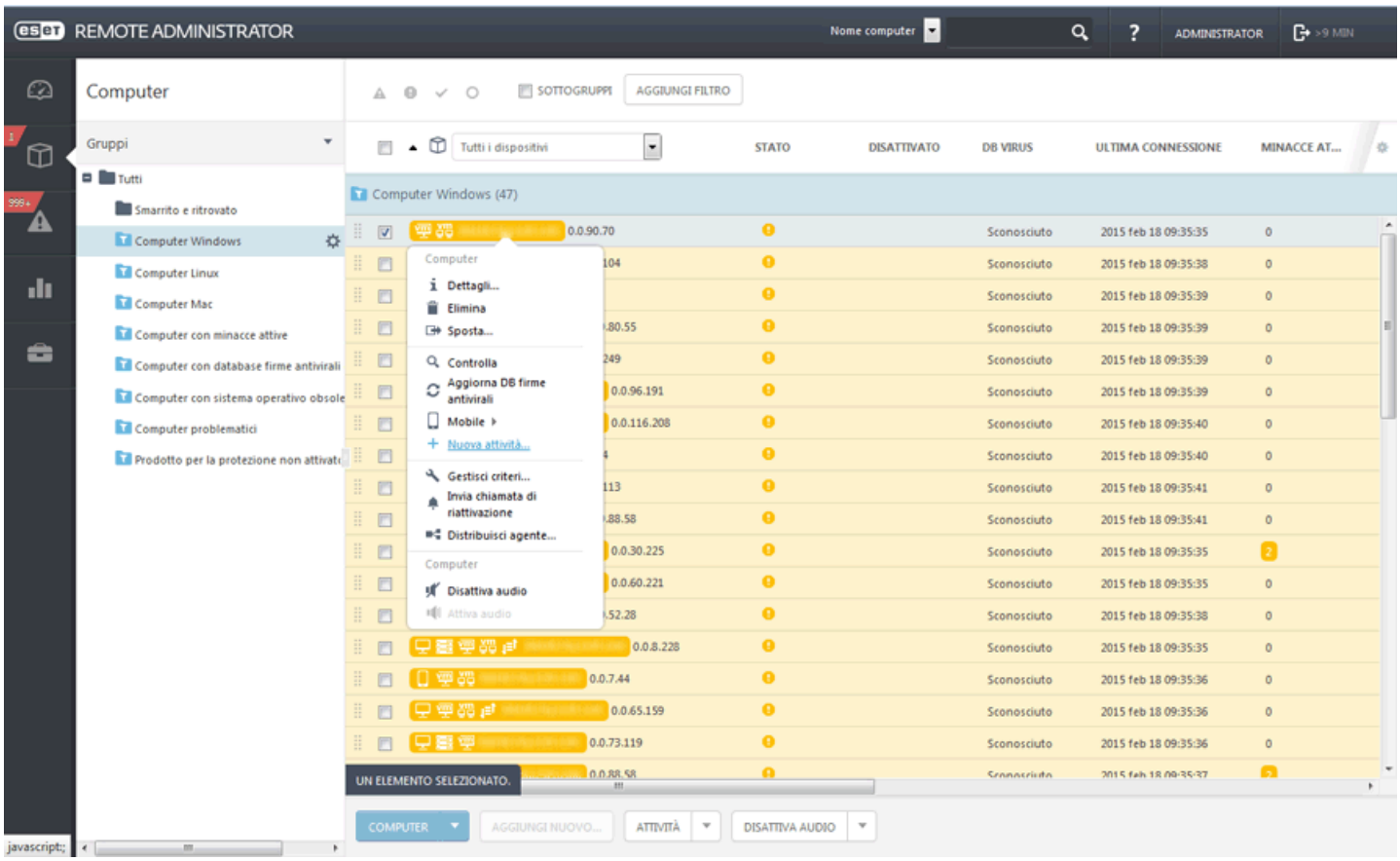
6.1.3.5 Assegna attività a uno o più computer

Un'attività può essere assegnata a uno o più computer in diversi modi:

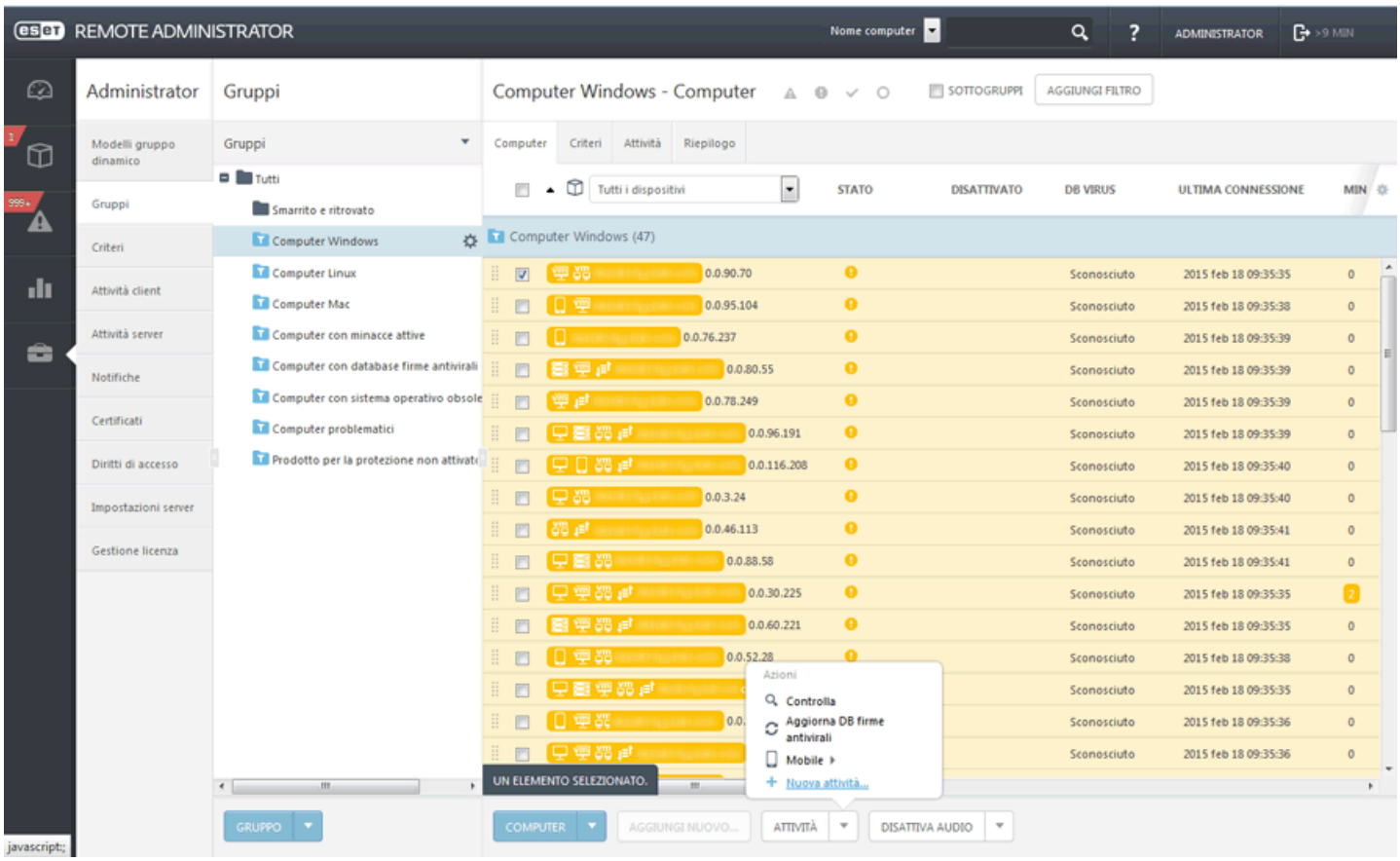
1. **Dashboard** > **Computer con problemi** > selezionare **+ Nuova attività...**



2. **Computer** > selezionare i computer tramite le caselle di controllo > selezionare + **Nuova attività...**



3. **Amministrazione**> **Gruppi** > selezionare i computer > pulsante **Attività**, selezionare un'azione e fare clic su + **Nuova attività...**



Verrà visualizzata una finestra della Procedura guidata nuova attività client.

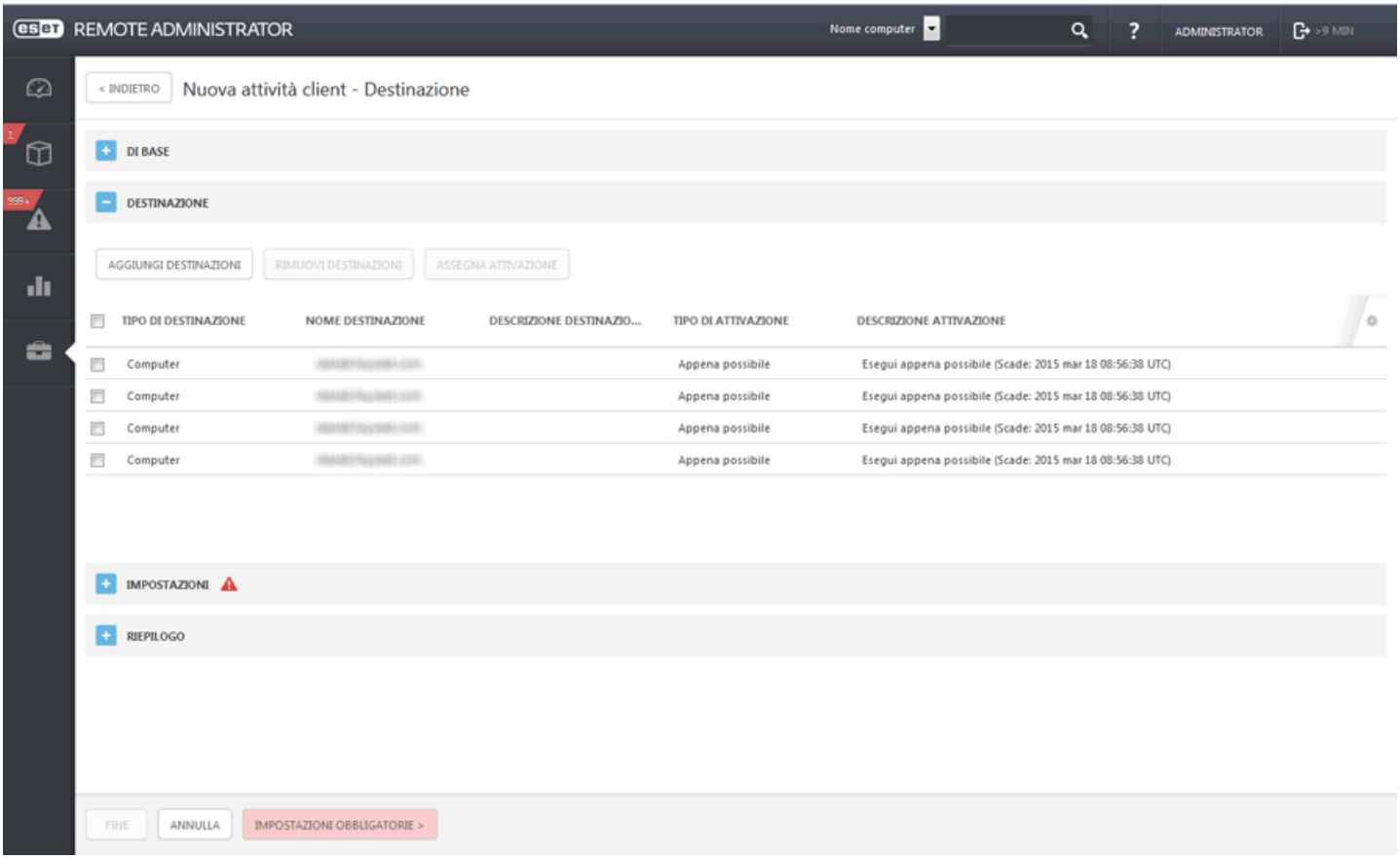
6.1.3.6 Pianifica un'attività

Per creare un'attività pianificata, procedere come descritto di seguito:

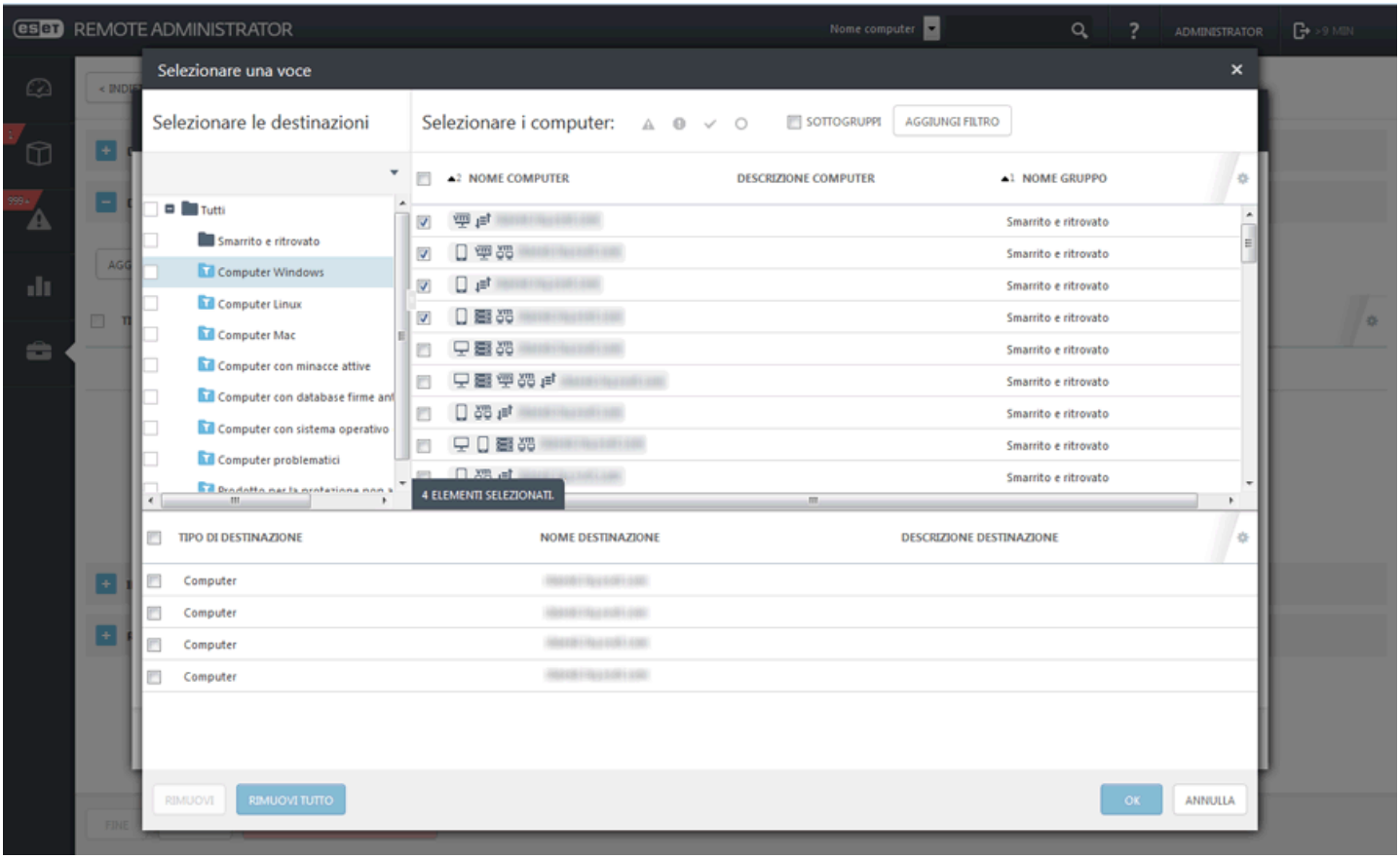
Accedere ad **Amministrazione** > **Attività client** > selezionare **Attività** e scegliere **Modifica...** accedere a **Destinazione**.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

6.1.3.7 Attivazioni

Le attivazioni possono essere utilizzate sia sul server sia sugli agenti ERA (client).

6.1.4 Attività server

Le attività server consentono di automatizzare le operazioni di routine. Sulle attività server possono essere configurate Attivazioni, ovvero l'attività verrà eseguita non appena sul server ERA si verifica una determinata combinazione di eventi.

Il server ERA può pianificare una delle seguenti attività:

- Sincronizzazione di gruppi statici che consente di aggiornare le informazioni dei client nei gruppi in modo da permettere all'utente di utilizzare dati aggiornati.
- Distribuzione agente per distribuire l'agente sui computer client.
- Genera report per generare report quando necessario.

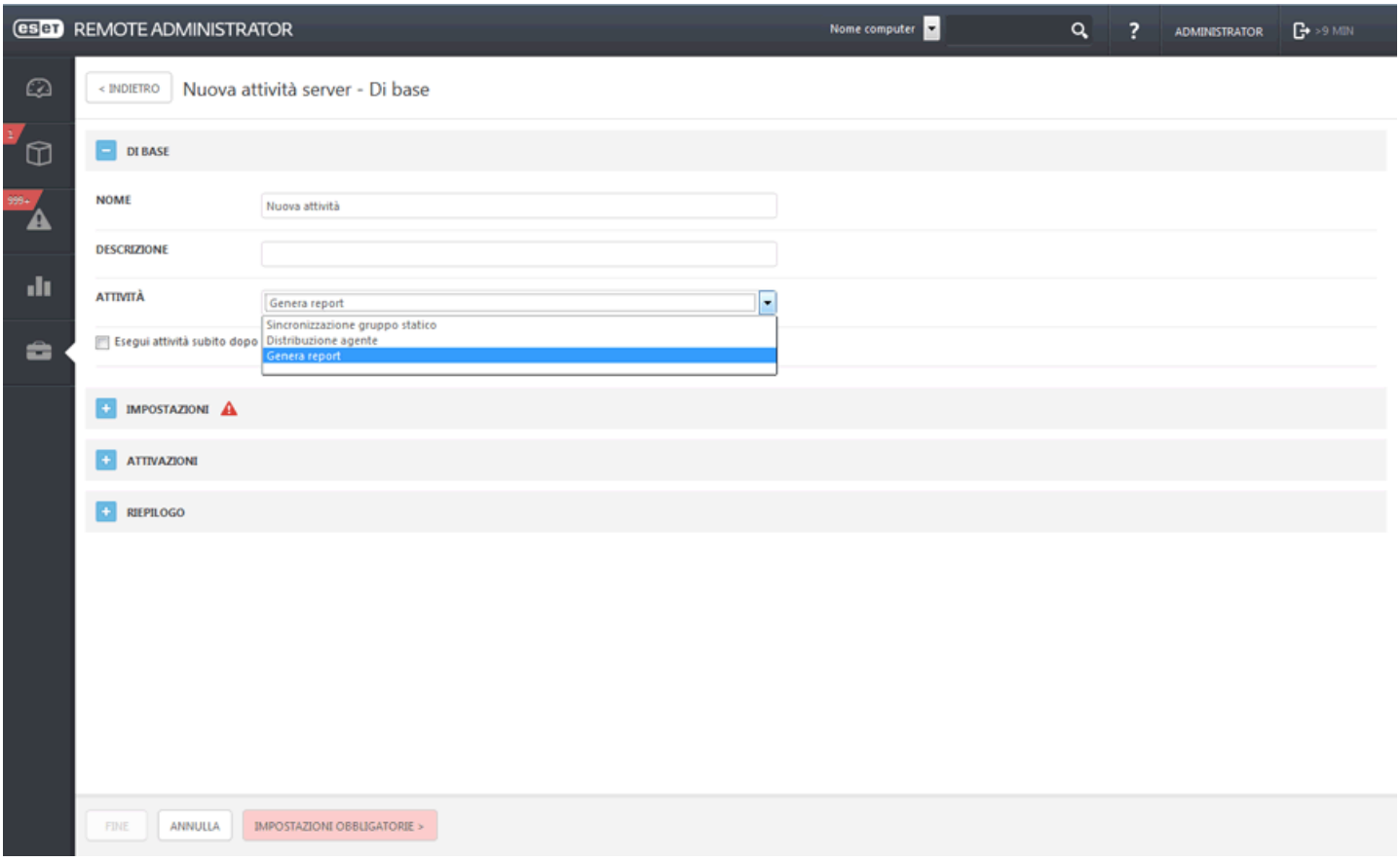
NOTA: le attività server non possono essere assegnate a client o gruppi di client specifici.

6.1.4.1 Procedura guidata attività server

Per iniziare a creare una nuova attività, fare clic su **Amministrazione** > **Attività server** > **Nuovo**.

Di base

Inserire le informazioni di base sull'attività, come il **Nome**, la **Descrizione** (facoltativa) e il **Tipo di attività**. Il **Tipo di attività** definisce le impostazioni e il comportamento dell'attività. Selezionare la casella di controllo accanto a Esegui attività subito dopo il termine per eseguire automaticamente l'attività dopo aver fatto clic su Fine.



6.1.4.2 Gestisci attività server

Le seguenti Attività server sono predefinite:

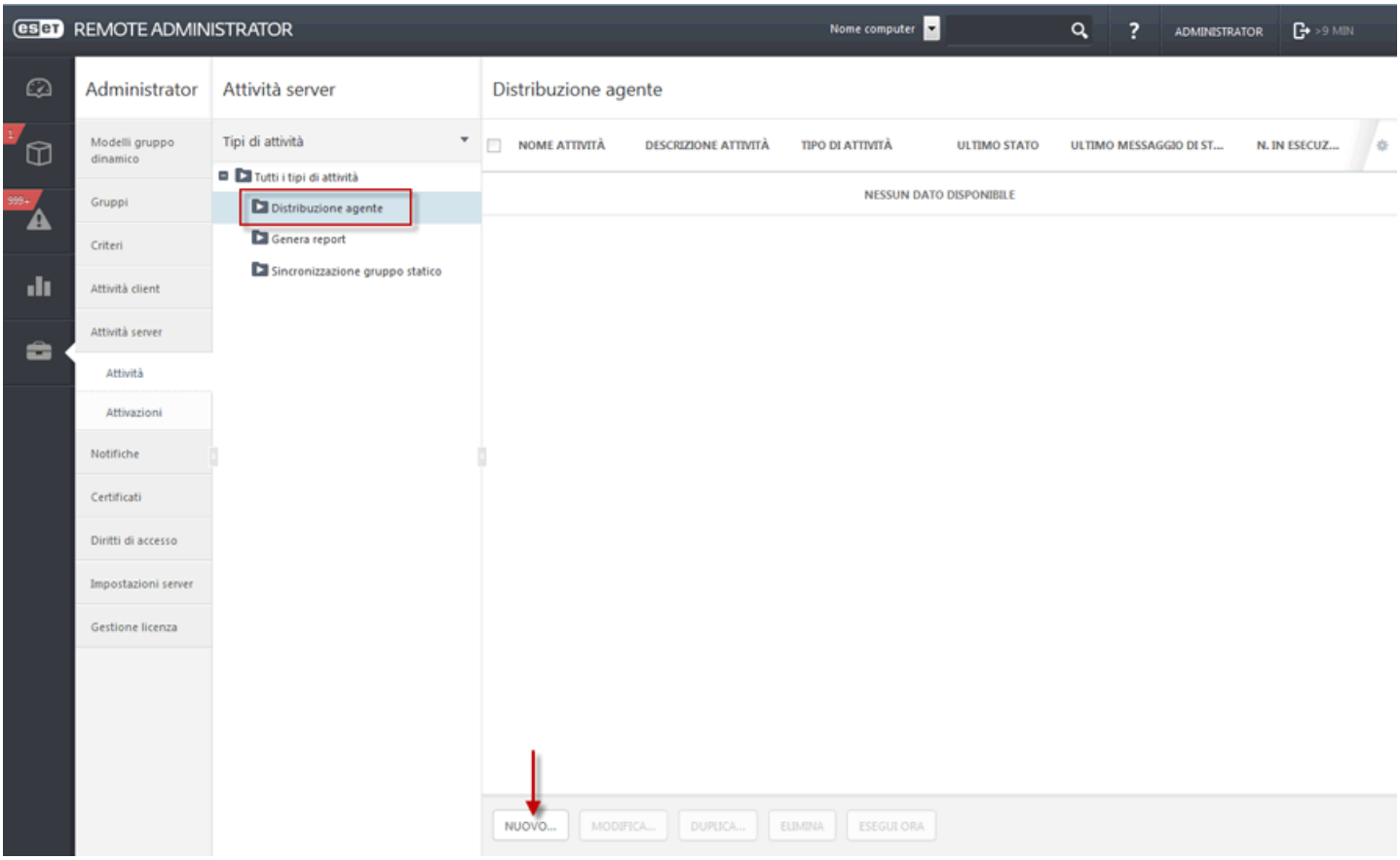
- Sincronizzazione dei gruppi statici che consente di aggiornare le informazioni dei gruppi per visualizzare le informazioni correnti.
- Distribuzione agente per distribuire l'agente sui computer client.
- Genera report per generare report quando necessario.

6.1.4.2.1 Distribuzione agente

La distribuzione da remoto dell'agente ERA viene eseguita dalla sezione **Amministrazione**. Utilizzare le istruzioni che seguono oppure guardare il video illustrativo della Knowledge Base.

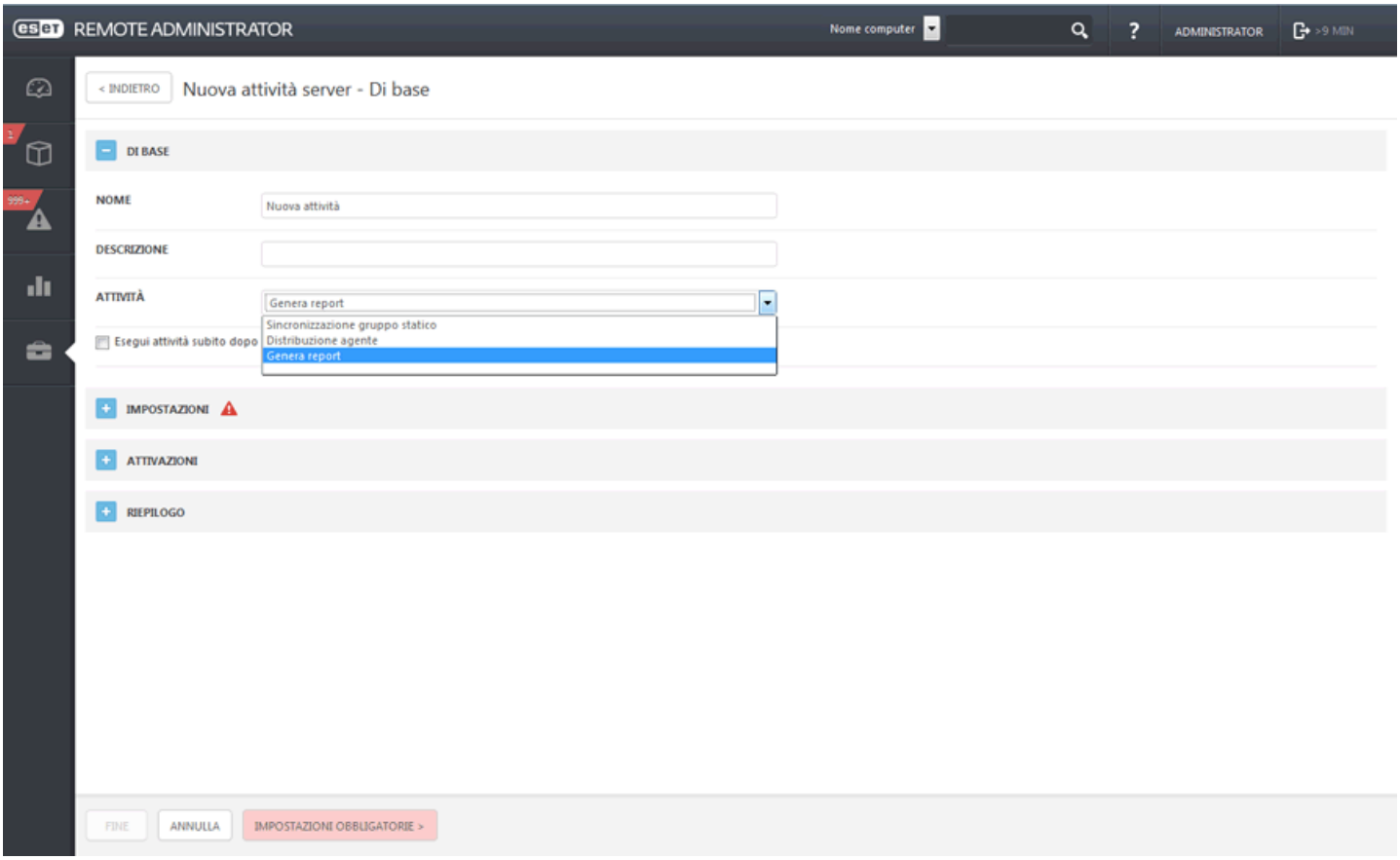
NOTA: si consiglia di testare dapprima la distribuzione di massa dell'agente nell'ambiente d'uso. Dopo averne garantito un corretto funzionamento, è possibile avviarne la distribuzione effettiva sui computer client degli utenti. Inoltre, prima di avviare i test sulla distribuzione di massa, modificare l'Intervallo di connessione dell'agente.

Fare clic su **Attività server** > **Distribuzione agente** > **Nuova...** per avviare la configurazione della nuova attività.



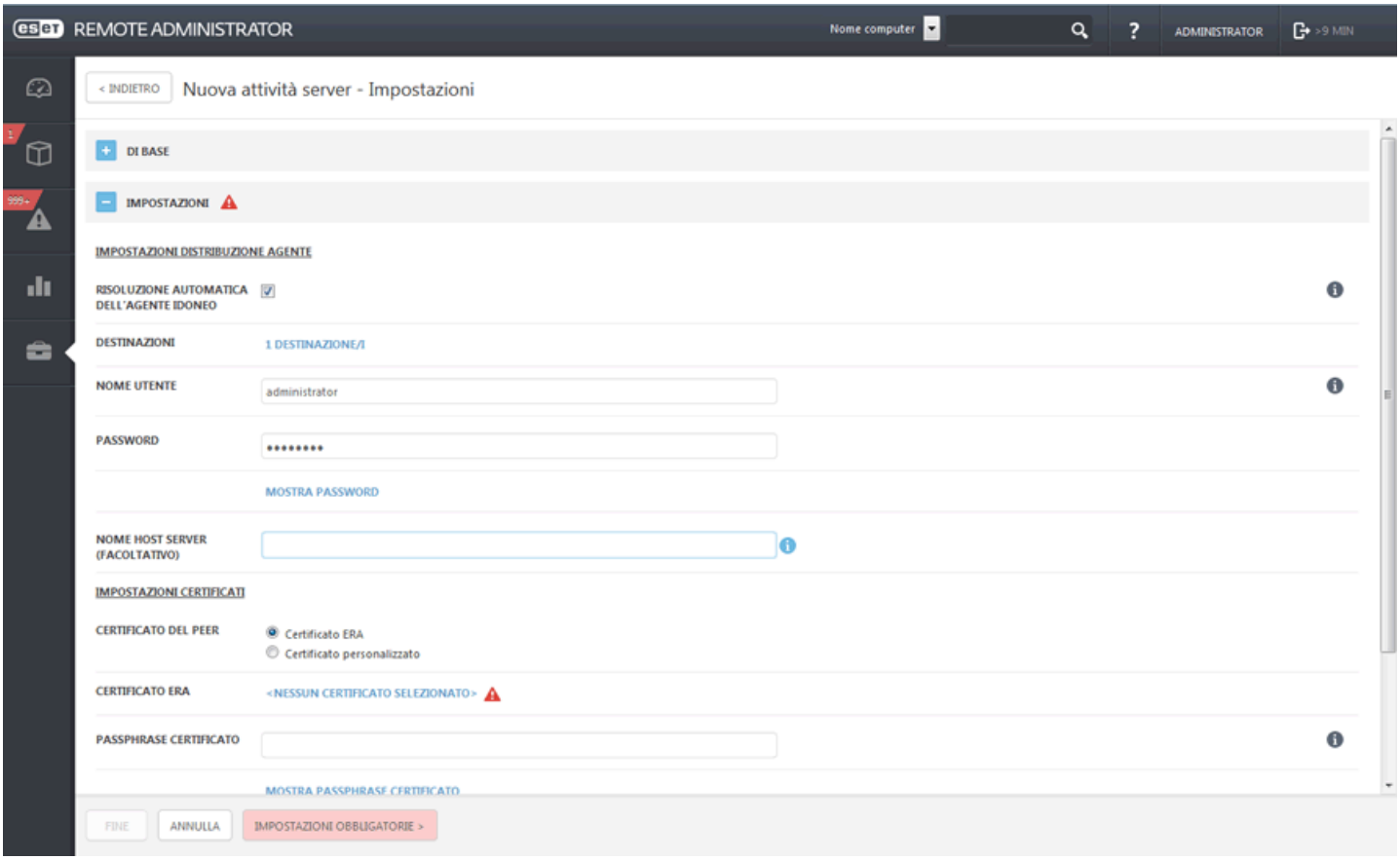
Di base

Inserire le informazioni di base sull'attività, come il **Nome**, la **Descrizione** (facoltativa) e il **Tipo di attività**. Il **Tipo di attività** definisce le impostazioni e il comportamento dell'attività. Selezionare la casella di controllo accanto a Esegui attività subito dopo il termine per eseguire automaticamente l'attività dopo aver fatto clic su Fine.



Impostazioni

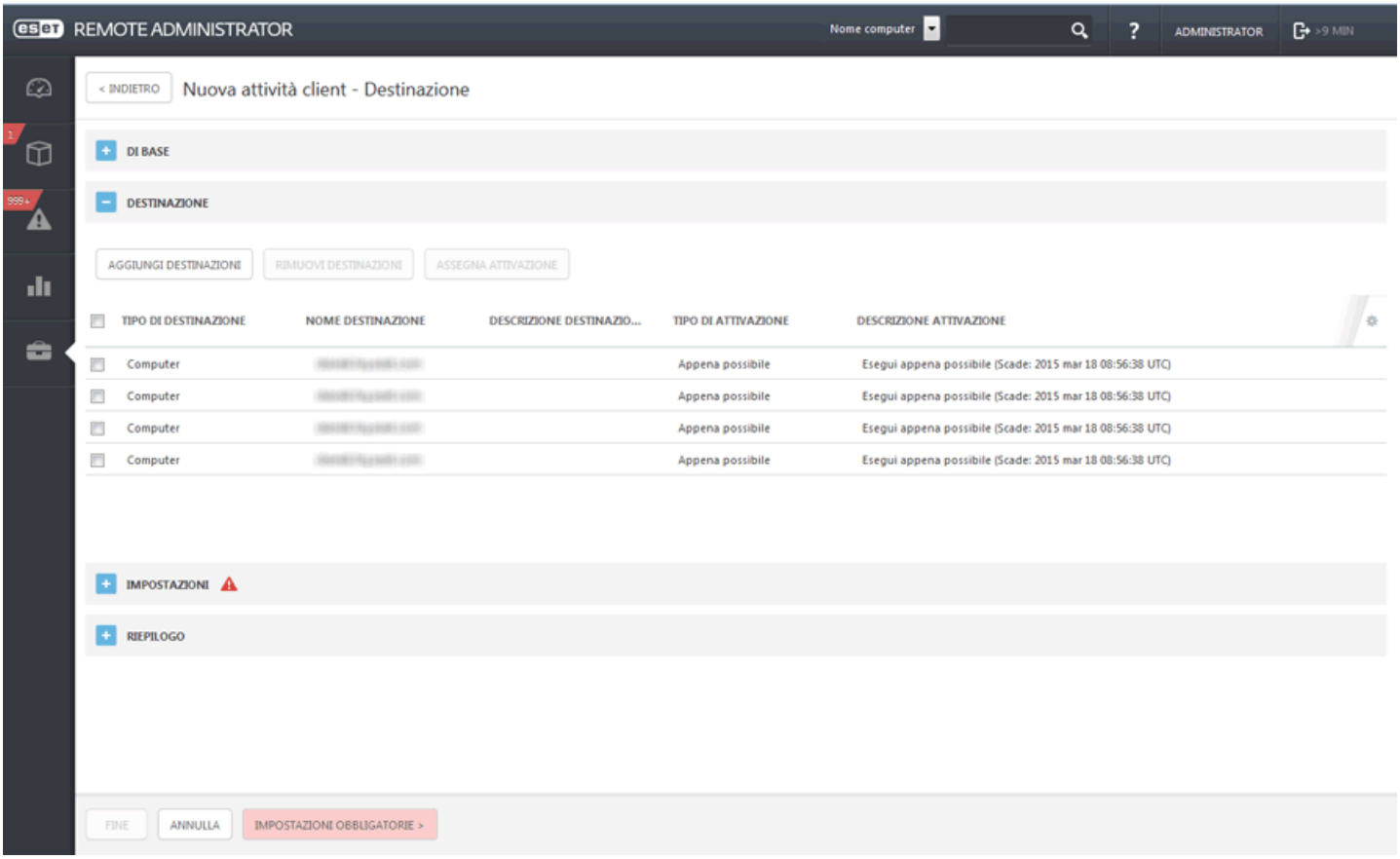
- **Risoluzione automatica dell'agente idoneo**: in presenza di più di un sistema operativo (Windows, Linux, Mac OS) nella rete, dopo aver selezionato questa opzione, l'attività troverà automaticamente il pacchetto di installazione dell'agente appropriato e compatibile con il server per ciascun sistema.
- **Destinazioni**: fare clic per selezionare i client destinatari dell'attività.
- **Nome utente/Password**: nome utente e password dell'utente con diritti sufficienti a eseguire un'installazione remota dell'Agente.
- **Nome host server (facoltativo)**: è possibile inserire un nome host del server, qualora quello sul lato client differisca da quello sul lato server.
- **Certificato del peer/Certificato ERA**: certificato di protezione e autorità di certificazione per l'installazione dell'Agente. È possibile selezionare il certificato predefinito e l'autorità di certificazione oppure utilizzare certificati personalizzati. Per ulteriori informazioni, consultare il capitolo Certificati.
- **Certificato personalizzato**: in caso di utilizzo di un certificato personalizzato per l'autenticazione, accedere al certificato e selezionarlo durante l'installazione dell'agente.
- **Passphrase certificato**: password per il certificato, che corrisponde a quella inserita dall'utente durante l'installazione del server (nel passaggio relativo alla creazione di un'autorità di certificazione) o a quella relativa al certificato personalizzato.



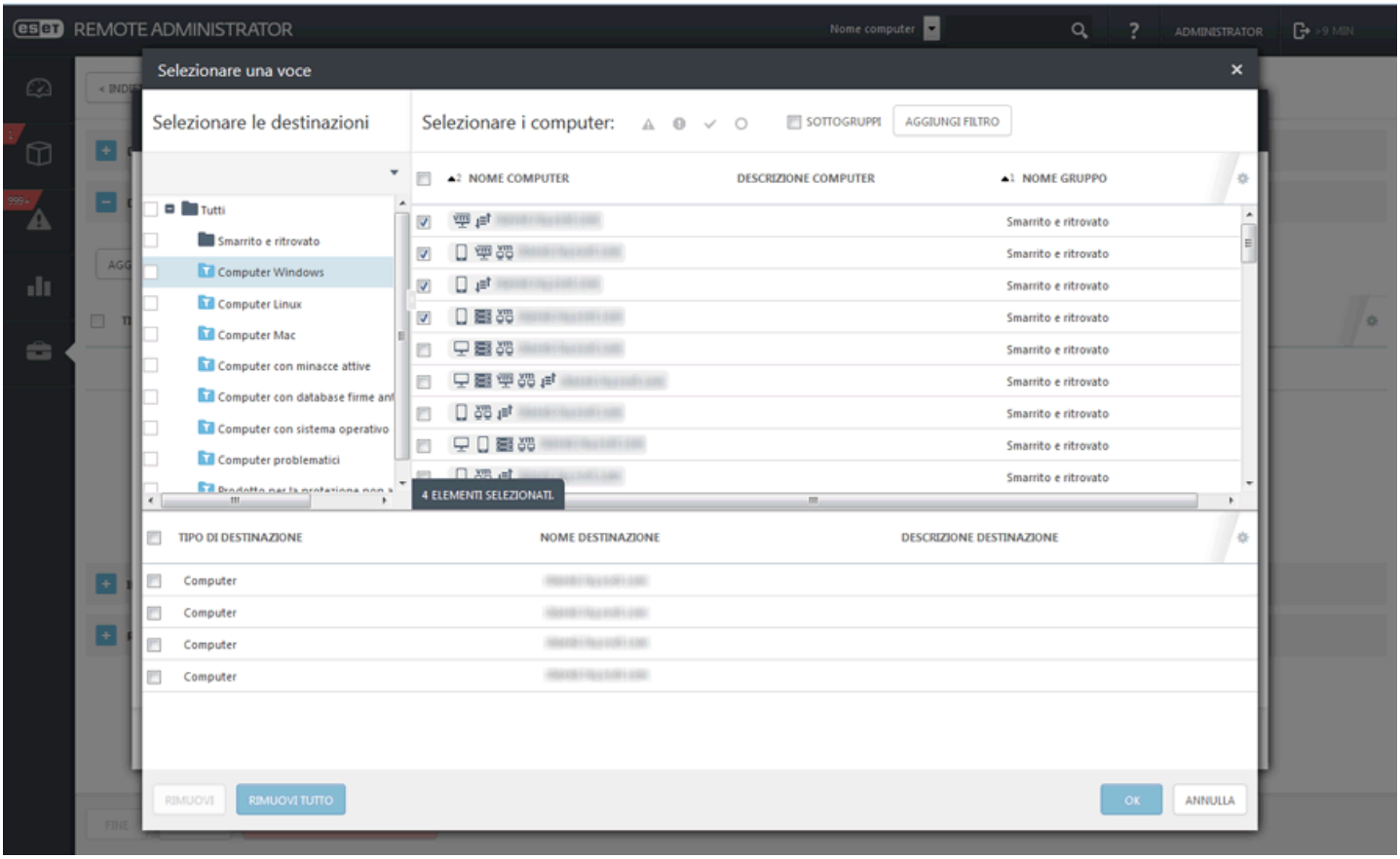
NOTA: il server ERA seleziona automaticamente il pacchetto di installazione dell'agente appropriato per i vari sistemi operativi. Per scegliere manualmente un pacchetto, deselezionare **Risoluzione automatica dell'agente idoneo** e scegliere il pacchetto che si desidera utilizzare nell'elenco di agenti disponibili nell'archivio ERA.

Destinazione

Qui è possibile specificare i client (computer singoli o interi gruppi) destinatari dell'attività.



Fare clic su **Aggiungi destinazioni** per visualizzare tutti i gruppi statici e dinamici e i relativi membri.



Selezionare i client, fare clic su **OK** e procedere alla sezione Attivazione.

Attivazione: determina l'evento che attiva l'attività.

- **Attivazione pianificata**: esegue l'attività a un orario specificato. È possibile pianificare l'attività una volta, ripetutamente oppure utilizzare un'Espressione CRON.
- **Appena possibile**: esegue l'attività non appena il client si connette al server ESET Remote Administrator e riceve l'attività. Se non è possibile eseguire l'attività entro la **Data di scadenza**, questa verrà rimossa dalla coda. Ciò non significa che verrà eliminata, ma solo che non verrà eseguita.
- **Attivazione rapporto eventi**: esegue l'attività in base agli eventi specificati qui. L'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Definire il **tipo di rapporto**, l'**operatore logico** e i criteri di **filtraggio** che attiveranno l'attività.
- **Attivazione gruppo dinamico aggiunto**: questa attivazione esegue l'attività nel momento in cui un client si aggiunge al gruppo dinamico selezionato nell'opzione di destinazione. Se è stato selezionato un Gruppo statico o uno o più client individuali, questa opzione non è disponibile.

NOTA: per ulteriori informazioni sulle attivazioni, consultare il capitolo Attivazioni.

Impostazioni avanzate: limitazione delle richieste: la limitazione delle richieste viene utilizzata per limitare l'esecuzione di un'attività attivata da un evento che si verifica con una certa frequenza, ad esempio l'**Attivazione rapporto eventi** o l'**Attivazione gruppo dinamico aggiunto** (v. paragrafo precedente). Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Fare clic su **Fine** dopo aver definito i destinatati dell'attività e le attivazioni che eseguono l'attività medesima.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

La distribuzione dell'agente può essere eseguita in modi diversi. L'agente può essere distribuito:

Da remoto, utilizzando un'attività server per la distribuzione di massa dell'agente ERA; in alternativa, è possibile effettuare la distribuzione dell'agente mediante GPO e SCCM
Localmente: attraverso l'utilizzo di un pacchetto di installazione dell'agente o i programmi di installazione live dell'agente, ad esempio se si verificano problemi durante la distribuzione remota

La distribuzione locale può essere eseguita in tre modi:

- Programmi di installazione live dell'agente: attraverso l'utilizzo di uno script generato dall'interno di ERA Web Console, è possibile effettuare la distribuzione dei programmi di installazione live dell'agente tramite e-mail oppure eseguirli da un supporto rimovibile (memoria USB e così via)
- Installazione assistita dal server: attraverso l'utilizzo del pacchetto di installazione dell'agente, i certificati vengono scaricati automaticamente dal server ERA (consigliato metodo di distribuzione locale)
- Installazione off-line: attraverso l'utilizzo del pacchetto di installazione dell'agente, è necessario esportare manualmente i certificati e utilizzarli in questo metodo di distribuzione

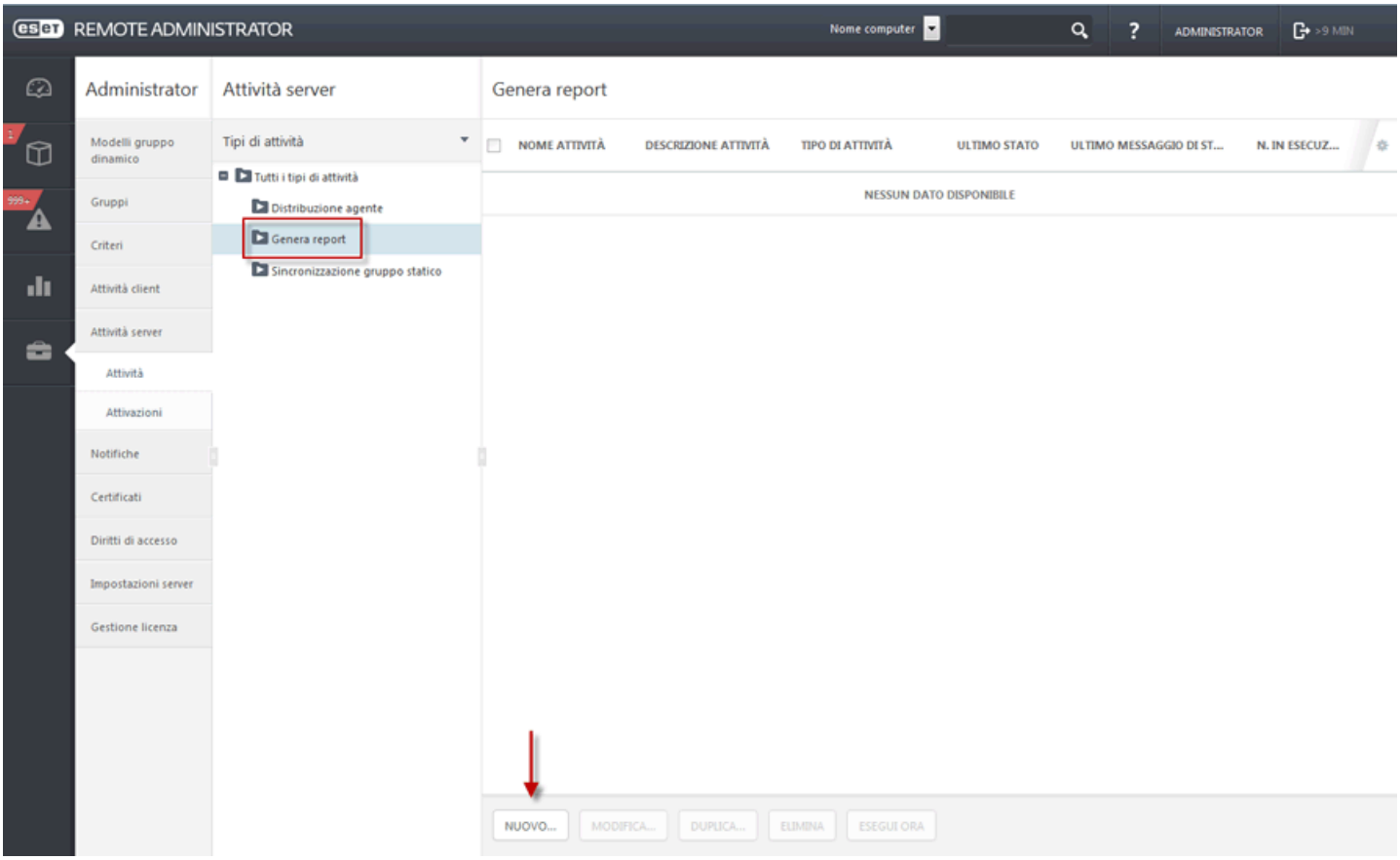
L'attività del server relativa alla distribuzione dell'agente da remoto può essere utilizzata per la distribuzione di massa dell'agente ai computer client. Grazie alla possibilità di eseguirlo dalla console Web senza la necessità di distribuire manualmente l'agente su ciascun computer, questo metodo rappresenta la soluzione di distribuzione più appropriata.

Dal momento che le soluzioni di protezione ESET in esecuzione sui computer client comunicano con il server ERA esclusivamente tramite l'agente, l'agente ERA si rivela una risorsa estremamente importante.

NOTA: in caso di problemi con la distribuzione dell'agente ERA da remoto (l'attività server **Distribuzione agente** non riesce), consultare la guida Risoluzione dei problemi.

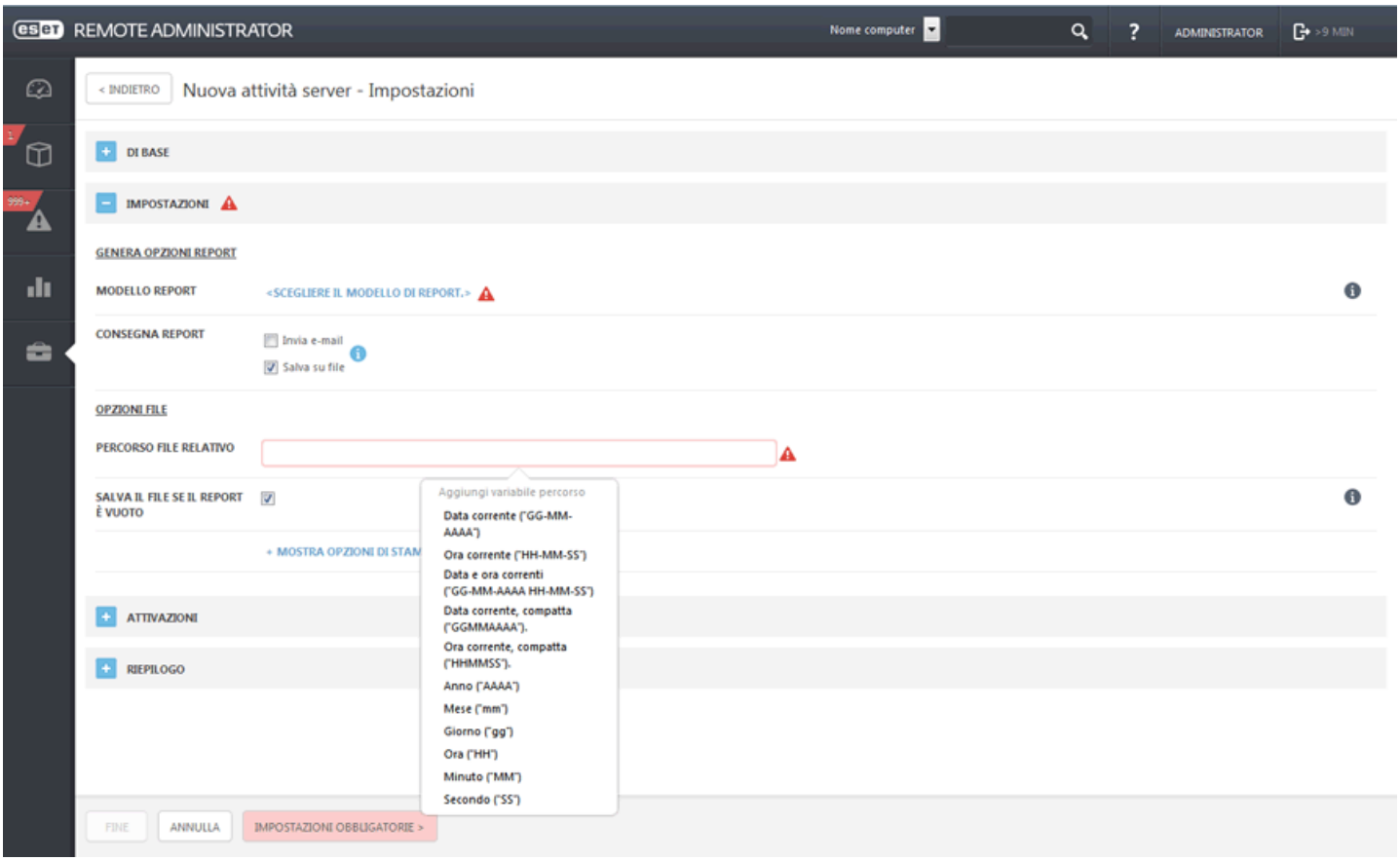
6.1.4.2.2 Genera report

L'attività **Genera report** viene utilizzata per generare report da Modelli di report creati precedentemente o predefiniti.



Impostazioni

Modello report: scegliere un modello report dall'elenco.



Selezionare Invia e-mail o Salva su file per ottenere il report generato.

INVIA E-MAIL

Per inviare/ricevere messaggi di posta, è necessario configurare le impostazioni SMTP in Impostazioni server > Impostazioni avanzate.

Messaggio di posta

- **Invia a**: immettere l'indirizzo o gli indirizzi e-mail dei destinatari del report. Separare gli indirizzi con una virgola (,). È anche possibile aggiungere i campi CC e CCN (funzionano esattamente allo stesso modo per i client di posta).
- **Oggetto**: oggetto del messaggio contenente il report. Immettere un oggetto riconoscibile in modo che i messaggi in entrata possano essere archiviati. Si tratta di un'impostazione facoltativa ma è consigliabile non lasciare il campo vuoto.
- **Contenuti messaggio**: definire il corpo del messaggio del report.
- **Invia e-mail se il report è vuoto**: utilizzare questa opzione se si desidera inviare il report anche se non contiene dati.

Opzioni di stampa

Fare clic su **Mostra opzioni di stampa** per visualizzare le seguenti impostazioni:

- **Formato output**: selezionare il formato del file appropriato. Il report generato, che verrà allegato al messaggio, potrà essere stampato in un momento successivo.
- **Lingua output**: selezionare la lingua per il messaggio. La lingua predefinita è quella selezionata per ERA Web Console.
- **Dimensioni pagina/Risoluzione/Orientamento foglio/Formato colore/Unità margine/Margini**: queste opzioni sono utili nel caso in cui si desideri stampare il report. Selezionare le opzioni appropriate in base alle preferenze di stampa. Queste opzioni valgono solo per il formato PDF e PS e non per il formato CSV.

NOTA: l'attività **Genera report** consente all'utente di selezionare diversi formati di file di output. Se si seleziona CSV, i valori della data e dell'ora nel report saranno archiviati nel formato UTC. Se invece si seleziona una delle due restanti opzioni di output (PDF, PS), nel report verrà utilizzata l'ora del server locale.

SALVA SU FILE

Opzioni file

- **Percorso file relativo**: il report verrà generato in una directory specifica, ad esempio: *C:\Users\All Users\ESET\RemoteAdministrator\Server\Data\GeneratedReports*
- **Salva file se il report è vuoto**: utilizzare questa opzione se si desidera salvare il report anche se non contiene dati.

Opzioni di stampa

Fare clic su **Mostra opzioni di stampa** per visualizzare le seguenti impostazioni:

- **Formato output**: selezionare il formato del file appropriato. Il report generato, che verrà allegato al messaggio, potrà essere stampato in un momento successivo.
- **Lingua output**: selezionare la lingua per il messaggio. La lingua predefinita è quella selezionata per ERA Web Console.
- **Dimensioni pagina/Risoluzione/Orientamento foglio/Formato colore/Unità margine/Margini**: queste opzioni sono utili nel caso in cui si desideri stampare il report. Selezionare le opzioni appropriate in base alle preferenze di stampa. Queste opzioni valgono solo per il formato PDF e PS e non per il formato CSV.

NOTA: l'attività **Genera report** consente all'utente di selezionare diversi formati di file di output. Se si seleziona CSV, i valori della data e dell'ora nel report saranno archiviati nel formato UTC. Se invece si seleziona una delle due restanti opzioni di output (PDF, PS), nel report verrà utilizzata l'ora del server locale.

Attivazioni

Selezionare un'attivazione esistente per questa attività o creare una nuova attivazione. È inoltre possibile **Rimuovere** o **Modificare** un'attivazione selezionata.

Riepilogo

Tutte le opzioni configurate verranno visualizzate qui. Controllare che le impostazioni siano corrette, quindi fare clic su Fine. L'attività è ora creata e pronta all'uso.

NOTA: Ubuntu Server Edition richiede che siano installati **X Server** e **xinit** per il corretto funzionamento di Report Printer (PDF Reports).

```
sudo apt-get install server-xorg
sudo apt-get install xinit
startx
```

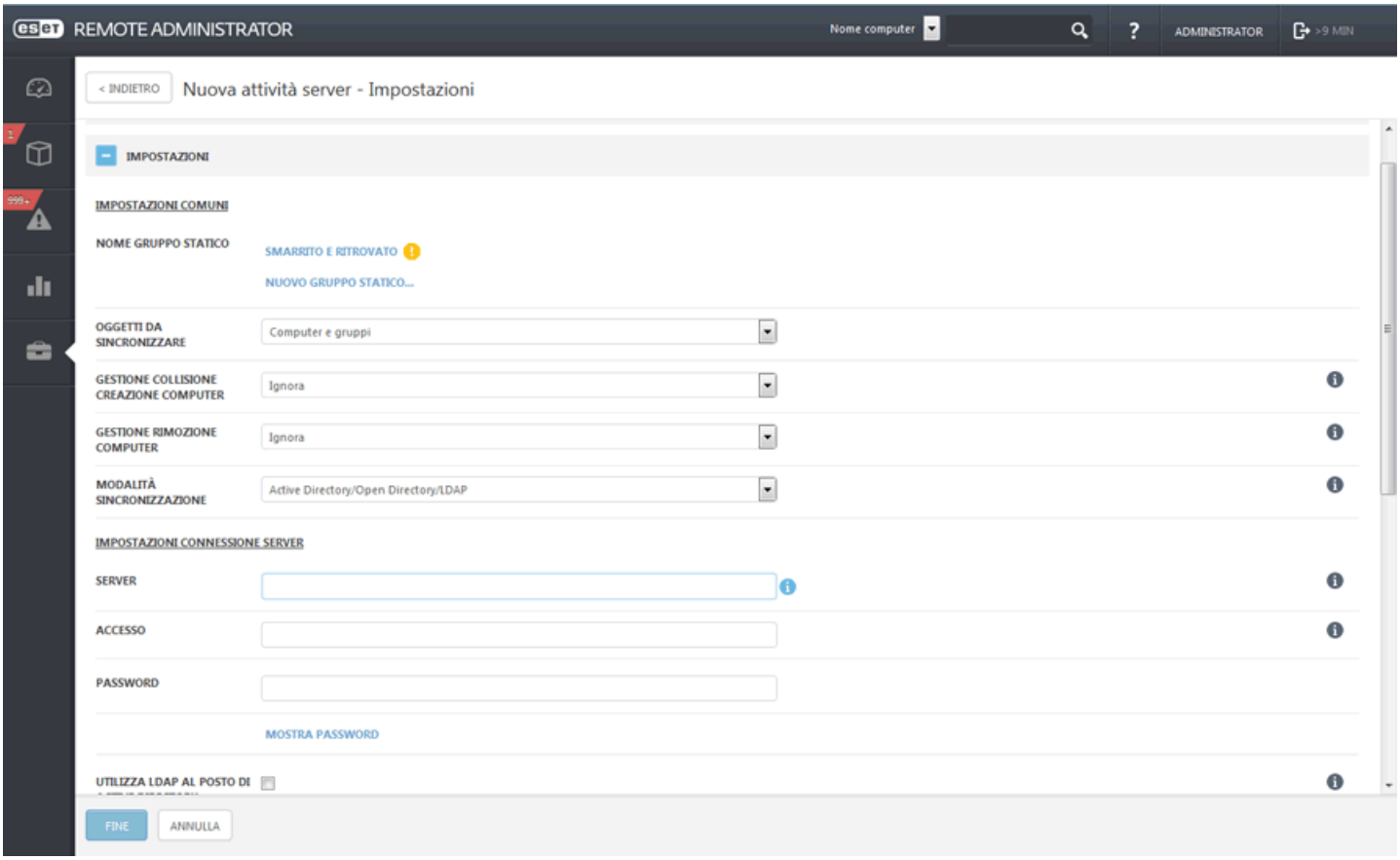
6.1.4.2.3 Sincronizzazione gruppo statico

L'attività **Sincronizzazione gruppo statico** eseguirà una ricerca all'interno della rete (Active Directory, Mac open Directory, LDAP, rete locale) dei computer e inserirà gli elementi trovati in un Gruppo statico. Se si seleziona **Sincronizza con Active Directory** durante l'Installazione del server, i computer rilevati verranno aggiunti al gruppo **Tutti**.

Fare clic su **Amministrazione** > **Attività server** >**Sincronizzazione gruppo statico** > **Nuova...** per avviare la configurazione della nuova attività.

Di base

Inserire le informazioni di base sull'attività, come il **Nome**, la **Descrizione** (facoltativa). Il **Tipo di attività** definisce le impostazioni e il comportamento dell'attività. Selezionare la casella di controllo accanto a Esegui attività subito dopo il termine per eseguire automaticamente l'attività dopo aver fatto clic su Fine.



Impostazioni

- **Nome gruppo statico**: questo gruppo sarà la radice per i computer sincronizzati.
- **Oggetto da sincronizzare**: **Computer e gruppi** o **Solo computer**.
- **Gestione collisione creazione computer**: se la sincronizzazione aggiunge computer che appartengono già al Gruppo statico, l'utente può selezionare un metodo di risoluzione dei conflitti. **Salta** (i computer sincronizzati non verranno aggiunti), **Sposta** (i nuovi computer verranno spostati in un sottogruppo) o **Duplica** (i nuovi computer verranno aggiunti con un nome differente).
- **Gestione rimozione computer**: se un computer non esiste più, è possibile **Rimuoverlo** o **Saltarlo**.

Modalità sincronizzazione:

- **Active Directory/Open Directory/LDAP:** immettere le **Informazioni sulla connessione del server** di base (nome server, dati di accesso, password).
- **Rete MS Windows:** immettere un **Gruppo di lavoro** da utilizzare e l'utente con le relative credenziali (dati di accesso e password).
- **VMware:** immettere il nome host o l'indirizzo IP e le credenziali utilizzate per accedere a VMware vCenter Server.

Impostazioni connessione server:

- **Server**: digitare il nome del server o l'indirizzo IP del controller di dominio.
- **Accesso**: digitare le credenziali di accesso del controller di dominio nel formato **dominio\nome utente**.
- **Password**: digitare la password utilizzata per accedere al controller di dominio.

- **Utilizza i parametri LDAP:** se si desidera utilizzare LDAP, selezionare la casella di controllo **Utilizza LDAP al posto di Active Directory** e inserire attributi specifici che corrispondono al server oppure selezionare una **Preimpostazione** facendo clic su **Personalizzata...** per inserire automaticamente gli attributi.

Impostazioni sincronizzazione:

- **Nome distinto**: percorso (Nome distinto) al nodo nella struttura Active Directory. Se si lascia vuota questa opzione, verrà eseguita la sincronizzazione all'intera struttura AD.
- **Nome/i distinto/i escluso/i**: l'utente può scegliere di escludere (ignorare) nodi specifici nella struttura Active Directory.
- **Computer disattivati ignorati (solo in Active Directory)**: l'utente può scegliere di ignorare i computer disabilitati in Active Directory. L'attività salterà tali computer.

Attivazioni

Selezionare un'attivazione esistente per questa attività o creare una nuova attivazione. È inoltre possibile **Rimuovere** o **Modificare** un'attivazione selezionata.

Riepilogo

Controllare le informazioni di configurazione visualizzate e, se corrette, fare clic su **Fine**. L'attività è ora creata e pronta all'uso.
Per impostazione predefinita, i destinatari sono solo i computer Windows. Se si utilizzano computer Linux in un dominio Windows e si desidera che siano i destinatari di questa attività, renderli prima visibili. I computer Linux in un dominio Windows non visualizzeranno alcun testo nelle proprietà computer ADUC (utenti e computer di Active Directory), quindi sarà necessario immettere manualmente queste informazioni.

6.1.4.2.4 Sincronizzazione gruppo statico - Computer Linux

I computer Linux uniti in un dominio Windows non visualizzeranno alcun testo nelle Proprietà computer degli utenti e dei computer di Active Directory (ADUC), quindi sarà necessario immettere manualmente queste informazioni.

- Controllare i Prerequisiti del server e i seguenti prerequisiti:

- I computer Linux si trovano in Active Directory.
- Sul controller di dominio è installato un server DNS.
- È installato **ADSI Edit**.

1. Aprire un prompt dei comandi ed eseguire adsiedit.msc
2. Accedere ad **Azione** > **Connetti a**. Verrà visualizzata la finestra delle impostazioni di connessione.
3. Fare clic su **Selezionare un contesto dei nomi noto**.
4. Espandere la casella combinata sottostante e selezionare il contesto dei nomi **Predefinito**.
5. Fare clic su **OK**: il valore ADSI sulla sinistra dovrebbe essere il nome del controller di dominio, il contesto dei nomi predefinito (il controller di dominio dell'utente).
6. Fare clic sul valore **ADSI** ed espanderne il sottogruppo.
7. Fare clic sul **sottogruppo** e accedere a NC (nome comune) oppure UO (unità organizzativa) dove sono visualizzati i computer Linux.
8. Fare clic sul **nome host** del computer Linux e selezionare **Proprietà** dal menu contestuale. Accedere al parametro **dNSHostName** e fare clic su **Modifica**.
9. Modificare il valore **<non impostato>** per convalidare il testo (ad esempio, *ubuntu.TEST*).

10. Fare clic su **OK** > **OK**. Aprire **ADUC** e selezionare le **proprietà** del computer Linux: il nuovo testo sarà visualizzato qui.

6.1.4.3 Pianificazione attività server

L'attivazione pianificata eseguirà l'attività in base a una data e a un orario impostati. L'attività può essere pianificata per essere **eseguita una volta**, eseguita ripetutamente oppure in base a un'espressione CRON.

6.1.4.4 Riutilizza attivazione in attività server

Se si riutilizza un'attivazione del server, la stessa attivazione (circostanza/evento) è in grado di avviare più attività (azioni) contemporaneamente.

Ad esempio, si immagini che un utente ERA abbia necessità di generare contemporaneamente 2 diversi report mensili periodici. Attenersi ai passaggi illustrati di seguito per riutilizzare l'attivazione per il primo report per creare il secondo.

1. Creare la prima attività Genera report con un'Attivazione pianificata ogni mese assegnata.
2. Iniziare a configurare la seconda attività Genera report con un report differente.
3. Nella schermata Attivazione della procedura guidata di creazione dell'attività fare clic su **Aggiungi** esistente. Verrà visualizzato l'elenco delle attivazioni esistenti.
4. Scegliere la stessa Attivazione pianificata ogni mese utilizzata per la prima attività Genera report.
5. **Salvare** l'attività. Dopo aver eseguito questi passaggi, i 2 report differenti verranno generati contemporaneamente ogni mese.

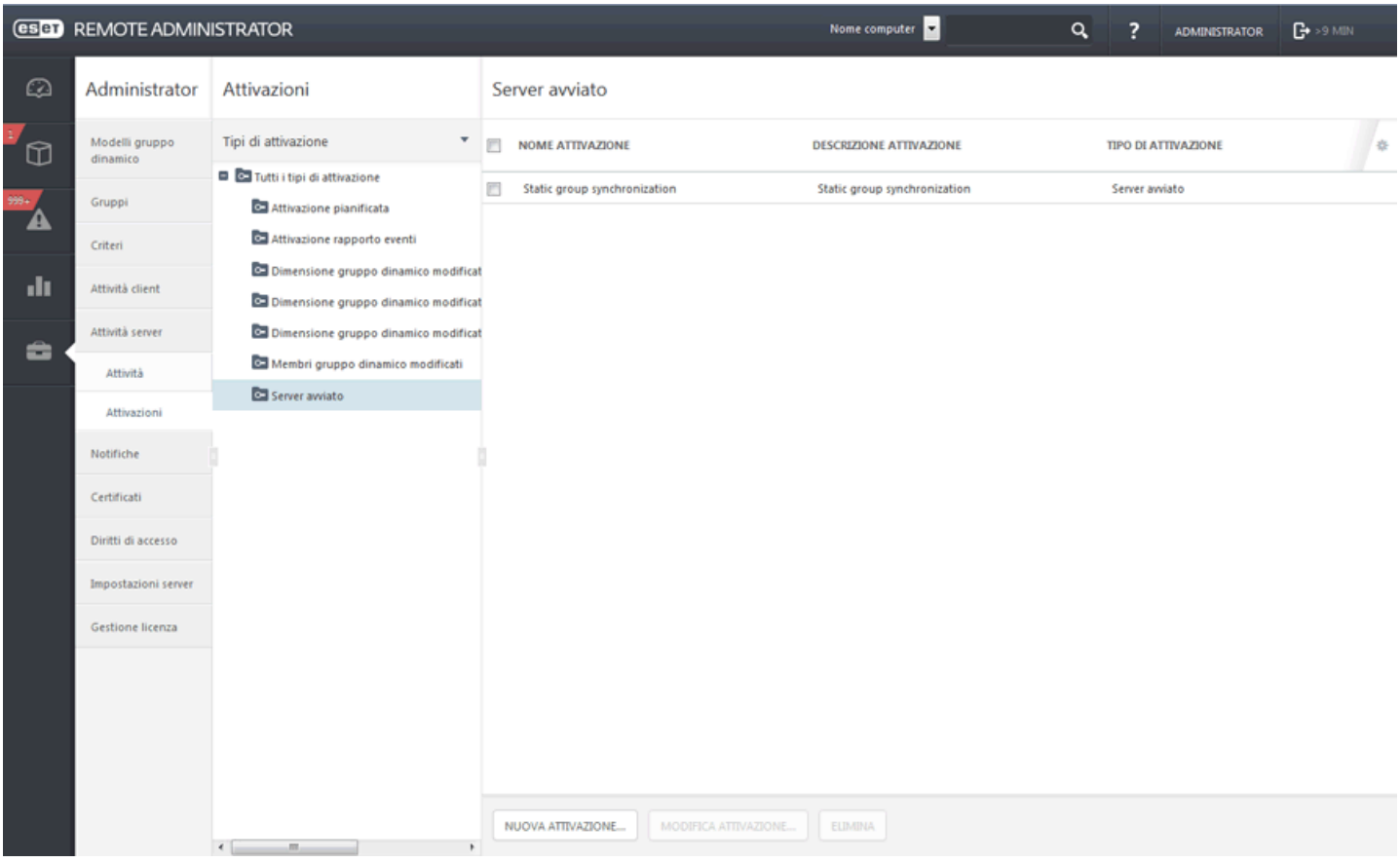
6.1.4.5 Attivazioni

Le attivazioni sono essenzialmente sensori che reagiscono a determinati eventi in maniera predefinita. Vengono utilizzate per eseguire un'azione (nella maggior parte dei casi per eseguire un'attività). Possono essere attivate dallo strumento di pianificazione attività (eventi temporali) o quando si verifica un determinato evento di sistema.

Un'attivazione esegue tutte le attività ad essa assegnate nel momento in cui viene attivata. L'attivazione non esegue immediatamente le attività appena assegnate: esse vengono eseguite non appena viene eseguita l'attivazione. È possibile ridurre ulteriormente la sensibilità delle attivazioni tramite la limitazione delle richieste.

Tipi di attivazione del server:

- **Membri gruppo dinamico modificati:** questa attivazione viene richiamata quando i contenuti di un Gruppo dinamico vengono modificati. Ad esempio, se i client entrano a far parte o escono da un Gruppo dinamico chiamato *Infetti*.
- **Dimensione gruppo dinamico modificata in base al gruppo confrontato:** l'attivazione viene richiamata quando il numero dei client in un Gruppo dinamico osservato viene modificato rispetto a un gruppo messo a confronto (statico o dinamico). Ad esempio, se più del 10% di tutti computer è infetto (il gruppo Tutti rispetto al gruppo Infetti).
- **Dimensione gruppo dinamico modificata in base alla soglia:** l'attivazione viene richiamata quando il numero dei client in un Gruppo dinamico è superiore o inferiore alla soglia specificata. Ad esempio, se nel gruppo Infetti sono presenti più di 100 computer.
- **Dimensione gruppo dinamico modificata in base al periodo di tempo:** l'attivazione viene richiamata quando il numero dei client in un Gruppo dinamico cambia in un determinato periodo di tempo. Ad esempio, se il numero di computer nel gruppo Infetti aumenta del 10% in un'ora.
- **Attivazione rapporto eventi:** l'attivazione viene richiamata al verificarsi di uno specifico evento nei rapporti. Ad esempio, se nel rapporto di controllo è presente una minaccia.
- **Attivazione pianificata:** l'attivazione viene richiamata a un orario e data specifici.
- **Server avviato:** viene richiamata all'avvio del server. Ad esempio, questa attivazione viene utilizzata per l'attività Sincronizzazione dei gruppi statici.



6.1.4.5.1 Limitazione delle richieste

In determinate circostanze, la limitazione delle richieste può impedire l'esecuzione di un'attivazione. Le condizioni basate sul tempo hanno precedenza rispetto a quelle statistiche.

Se viene soddisfatta una qualsiasi delle condizioni, tutte le informazioni sullo stato di tutti gli osservatori vengono ripristinate (l'osservazione parte da 0). Ciò vale sia per le condizioni basate sul tempo sia per le condizioni statistiche. Le informazioni sullo stato per gli osservatori non sono persistenti. Ciò significa che vengono ripristinate anche in caso di riavvio dell'agente o del server.

Qualsiasi modifica apportata a un'attivazione ne reimposta lo stato.

Le attivazioni possono essere controllate in vari modi:

Statistiche

Le attivazioni statistiche sono indotte da qualsiasi combinazione dei seguenti parametri:

- S1: l'attivazione dovrebbe essere eseguita ogni **N** occorrenze dell'evento di attivazione (modulo **N**) a partire dall'ultimo evento in una serie (ad esempio, dall'inizio attendere l'N° evento)
- S2: l'attivazione viene eseguita se **N** eventi si verificano entro **X volte** (il parametro può essere scelto da una serie predefinita) [**N** <= 100] in senso totale galleggiante, ovvero viene preso in considerazione solo il conteggio degli eventi durante la X volta. L'esecuzione dell'attivazione induce un ripristino del buffer
- S3: si verificano **N** eventi con un simbolo univoco **S** [N <= 100] in serie. Il buffer viene ripristinato se l'attivazione viene eseguita e se nel buffer è già presente un evento. Il buffer è nella modalità "finestra galleggiante": coda FIFO. Il nuovo simbolo viene messo a confronto con ogni simbolo nel buffer.
  Nota: un valore mancante (n/d) viene considerato come non univoco e, pertanto, il buffer viene ripristinato dall'ultima attivazione eseguita

Queste condizioni possono essere combinate all'operatore E (devono essere soddisfatte tutte quelle impostate) o all'operatore OPPURE (quella che si verifica per prima).

Basate sul tempo

È necessario che siano soddisfatte contemporaneamente tutte le seguenti condizioni (se impostate):

- T1: l'attivazione può essere eseguita entro un **intervallo di tempo X**. L'intervallo viene fornito come una serie ripetuta di orari marginali, ad esempio 13:00 - 14:00 OPPURE 17:00 - 23:30)
- T2: l'attivazione può essere eseguita al massimo ogni **X volte**.

Proprietà aggiuntive

Come specificato in precedenza, non tutti gli eventi possono indurre l'esecuzione di un'attivazione. Le azioni eseguite per gli eventi che non inducono l'esecuzione di attivazioni possono essere le seguenti:

- Se viene ignorato più di un evento, raggruppare gli ultimi **N** eventi in uno (archiviare i dati degli eventi eliminati) [**N** <= 100]
- per **N** == 0, viene elaborato solo l'ultimo evento (**N** indica la lunghezza della cronologia, l'ultimo evento viene sempre elaborato)
- Tutti gli eventi che non inducono un'attivazione vengono uniti (unione dell'ultimo evento con **N** eventi storici)

Esempi:

S1: criterio per le occorrenze (consentire ogni 3° evento)

Ora	00	01	02	03	04	05	06	l'attivazione viene modificata	07	08	09	10	11	12	13	14	15
Eventi	x	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: criterio per le occorrenze che si verificano entro l'orario (consentire se si verificano 3 eventi in 4 secondi)

Ora	00	01	02	03	04	05	06	l'attivazione viene modificata	07	08	09	10	11	12	13
Eventi	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: criterio per valori con simbolo univoco (consentire se sono presenti 3 valori univoci in serie)

Ora	00	01	02	03	04	05	06	l'attivazione viene modificata	07	08	09	10	11	12	13
Valore	A	B	B	C	D	G	H		J	K	n/d	L	M	N	N
S3					1									1	

S3: criterio per valori con simbolo univoco (consentire se sono presenti 3 valori univoci dall'ultimo evento)

Ora	00	01	02	03	04	05	06	07	l'attivazione viene modificata	08	09	10	11	12	13	14
Valore	A	B	B	C	D	G	H	I		J	K	n/d	L	M	N	N
S3				1			1						1			

T1: consentire un evento in un determinato intervallo di tempo (consentire ogni giorno a partire dalle 8:10, durata 60 secondi)

Ora	8:09:50	8:09:59	8:10:00	8:10:01	l'attivazione viene modificata	8:10:59	8:11:00	8:11:01
Eventi	x	x	x	x		x	x	x
T1			1	1		1		

Questo criterio non ha alcun stato: Le modifiche non hanno pertanto alcun effetto sui risultati.

T2: consentire un singolo evento in un intervallo di tempo (consentire al massimo ogni 5 secondi)

Ora	00	01	02	03	04	05	06	l'attivazione viene modificata	07	08	09	10	11	12	13
Eventi	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Combinazione S1+S2

- S1: ogni 5° evento
- S2: 3 eventi entro 4 secondi

Ora	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Eventi	x	x	x	x	x		x	x	x			x		x	x		
S1															1		

S2			1				1							1		
Risultato			1				1							1		

Il risultato viene enumerato come: S1 (o logico) S2

Combinazione S1+T1

- S1: consentire ogni 3° evento
- T1: consentire ogni giorno a partire dalle 8:08, durata 60 secondi

Ora:	**8:07:50**	**8:07:51**	**8:07:52**	**8:07:53**	**8:08:10**	**8:08:11**	**8:08:19**	**8:08:54**	**8:08:55**	**8:09:01**
Eventi	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
Risultato						1			1	

Il risultato viene enumerato come: S1 (e logico) T1

Combinazione S2+T1

- S2: 3 eventi entro 10 secondi
- T1: consentire ogni giorno a partire dalle 8:08, per una durata di 60 secondi

Ora:	**8:07:50**	**8:07:51**	**8:07:52**	**8:07:53**	**8:08:10**	**8:08:11**	**8:08:19**	**8:08:54**	**8:08:55**	**8:09:01**
Eventi	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Risultato							1			

Il risultato viene enumerato come: S2 (e logico) T1.
Si noti che lo stato di S2 viene ripristinato solo quando il risultato globale è 1.

Combinazione S2+T2

- S2: 3 eventi entro 10 secondi
- T2: consentire al massimo una volta ogni 20 secondi

Ora:	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**...**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
Eventi	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Risultato			1													1		

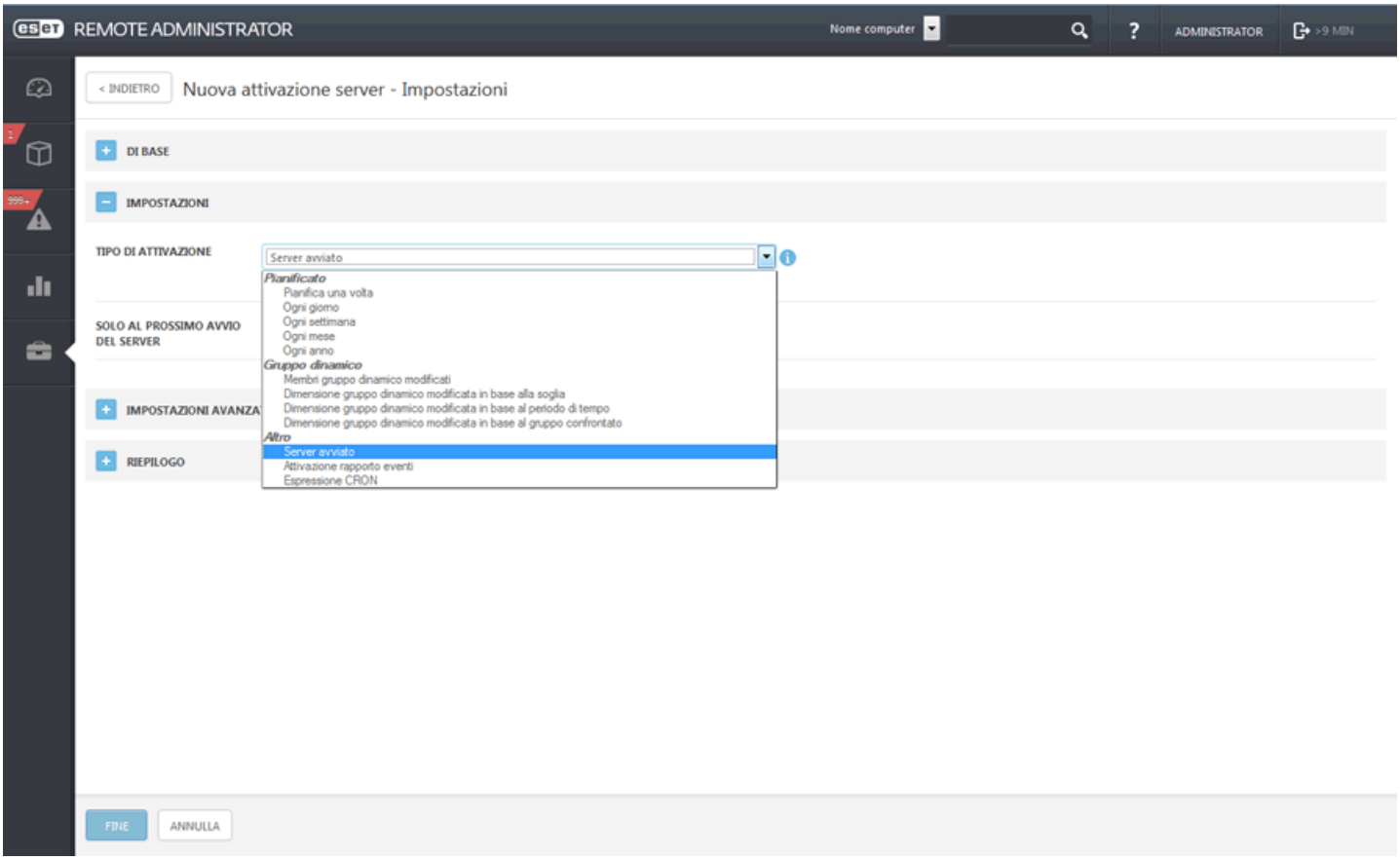
Il risultato viene enumerato come: S2 (e logico) T2.
Si noti che lo stato di S2 viene ripristinato solo quando il risultato globale è 1.

6.1.4.5.1.1 Eccessiva sensibilità dell'attivazione

Fare riferimento alle condizioni delle limitazioni delle richieste illustrate nella sezione Eccessiva esecuzione dell'attivazione di questa guida.

6.1.4.5.2 Procedura guidata attivazioni server

Le attivazioni sono create e gestite nella scheda **Amministrazione** > **Attività server** > **Attivazioni.** Selezionare **Tipo di attivazione** > **Nuova attivazione.**



6.1.4.5.3 Gestisci attivazioni server

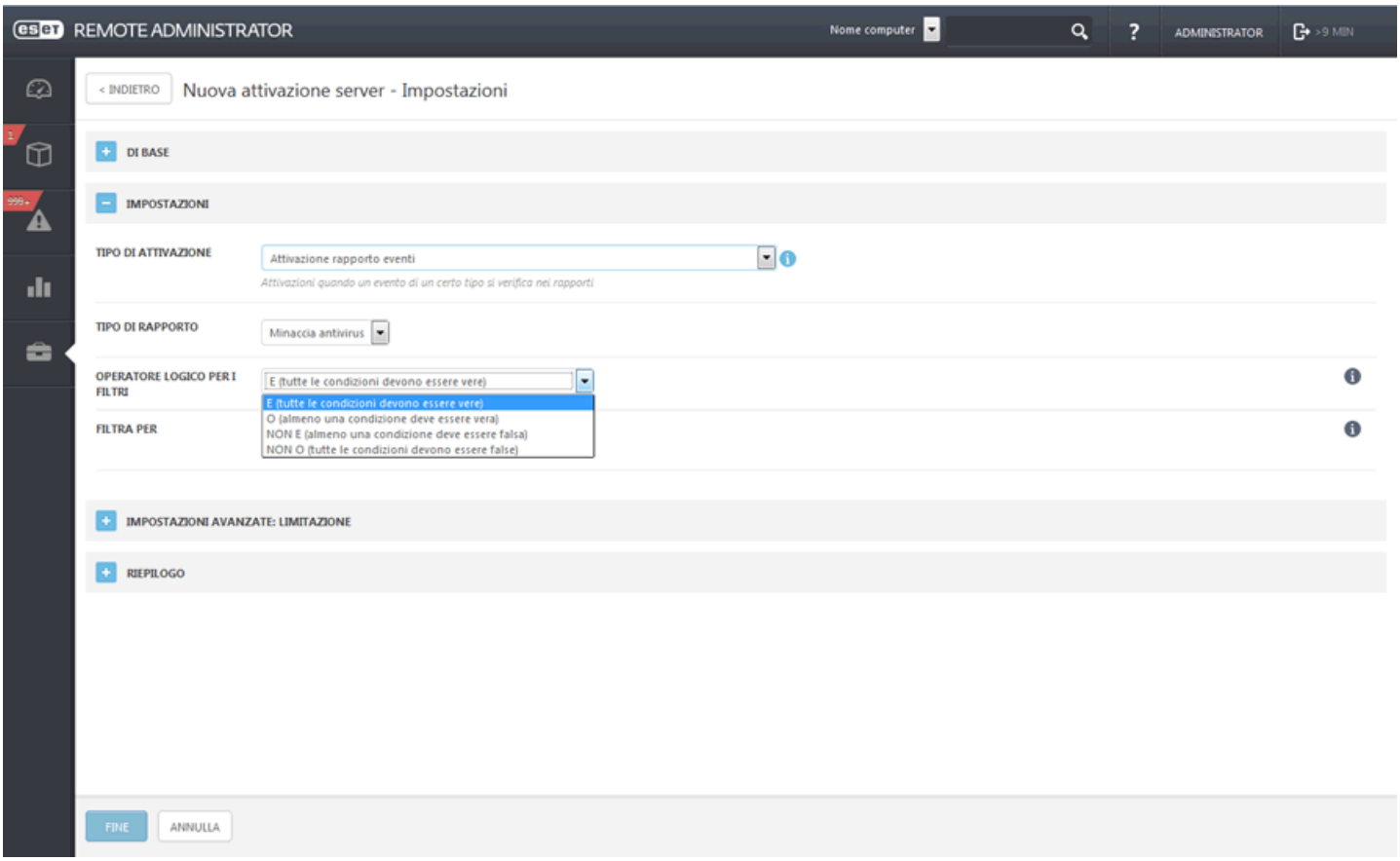
Per gestire le Attivazioni server, nella scheda **Amministrazione** fare clic su **Attività server** > **Attivazioni**, selezionare **Tipo di attivazione** e fare clic su **Modifica.**

Di base

Immettere un **nome** per l'attivazione. È anche possibile immettere una **descrizione** dell'attivazione, se desiderato.

Impostazioni

- Selezionare un tipo di attivazione. Il tipo di attivazione definisce il metodo di attivazione. Selezionare un'**Attivazione rapporto eventi** e continuare.
- Selezionare un **tipo di rapporto**. L'attivazione viene eseguita al verificarsi di uno specifico evento in questo rapporto.
- Definire l'evento che deve verificarsi per poter eseguire l'attivazione. Selezionare un **operatore logico** per filtrare gli eventi. Nell'esempio è stato selezionato **E (tutte le condizioni devono essere vere)**.
- Se necessario, aggiungere un **filtro** dall'elenco (come evento) e selezionare l'operatore logico per la stringa personalizzata.

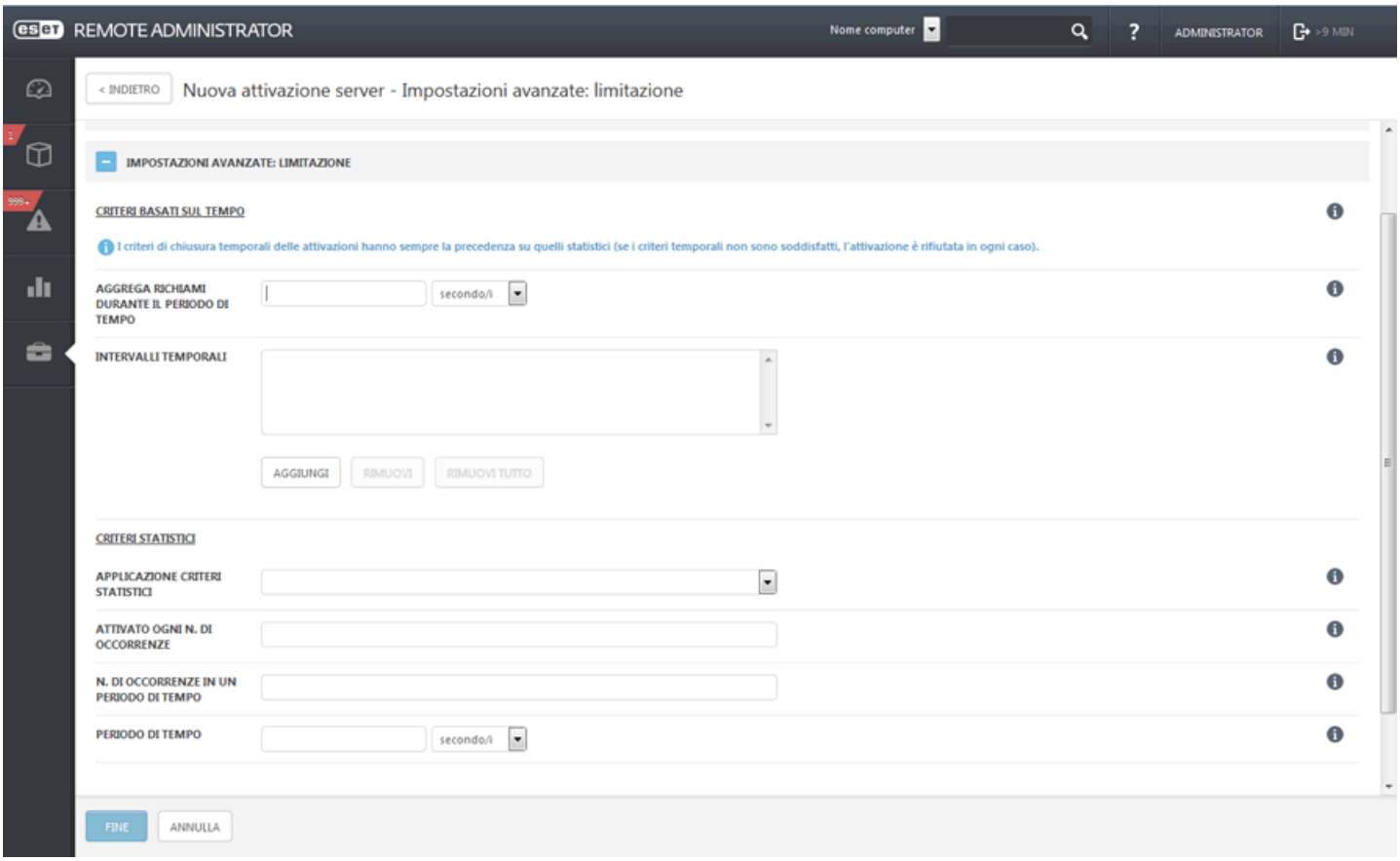


Selezionare un operatore logico nel menu **Operazione**.

- **E**: tutte le condizioni definite devono essere vere.
- **O**: almeno una condizione deve essere vera.
- **NON E**: almeno una condizione deve essere falsa.
- **NON O**: tutte le condizioni devono essere false.

Impostazioni avanzate: limitazione delle richieste

Specificare il **Numero di eventi da aggregare**. Questa opzione consente di definire il numero di eventi (risultati eventi) necessari per attivare l'invio della notifica. Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.



Riepilogo

Rivedere il riepilogo della nuova attivazione, apportare modifiche se necessario e fare clic su **Fine**. L'attivazione è ora salvata sul server e pronta per l'uso. Le attivazioni create sono anche visualizzate nell'elenco a destra. Per modificare o eliminare l'attivazione è sufficiente fare clic sull'attivazione nell'elenco e selezionare l'azione appropriata dal menu contestuale. Per eliminare contemporaneamente più attivazioni, selezionare le caselle di controllo accanto alle attivazioni che si desiderano rimuovere e fare clic su **Elimina**.

6.1.4.5.3.1 Eccessiva esecuzione dell'attivazione

Nel caso in cui l'utente desideri riceve notifiche con una minore frequenza, tenere presenti i seguenti suggerimenti:

- Se l'utente desidera reagire solo se si verificano più eventi e non un singolo evento, consultare la condizione statistica S1 nella sezione Limitazione delle richieste.
- Se l'attivazione deve essere eseguita solo se si verificano gruppi di eventi, attenersi alla condizione statistica S2 nella sezione Limitazione delle richieste.
- Quando gli eventi con valori indesiderati dovrebbero essere ignorati, consultare la condizione statistica S3 nella sezione Limitazione delle richieste.
- Quando gli eventi al di fuori degli orari di interesse (ad esempio l'orario di lavoro) dovrebbero essere ignorati, consultare la condizione basata sul tempo T1 nella sezioneLimitazione delle richieste.
- Per impostare un orario minimo tra l'esecuzione delle attivazioni, consultare la condizione basata sul tempo T2 nella sezione Limitazione delle richieste.

NOTA: le condizioni possono anche essere unite per formare scenari di limitazione delle richieste più complessi.

6.1.4.5.3.2 Espressione CRON

Un'espressione CRON viene utilizzata per configurare istanze specifiche di un'attivazione. È una stringa costituita da 7 sottoespressioni (campo) che rappresentano singoli valori della pianificazione. Questi campi sono separati da uno spazio e possono contenere uno qualsiasi dei valori consentiti con varie combinazioni.

Nome	Richiesto	Valore	Caratteri speciali consentiti
Secondi	Sì	0-59	,-*/
Minuti	Sì	0-59	,-*/
Ore	Sì	0-23	,-*/
Giorno del mese	Sì	1-31	,-*/ L W C
Mese	Sì	0-11 o GEN-DIC	,-*/
Giorno della settimana	Sì	1-7 or DOM-SAB	,-*/ L C #
Anno	No	vuoto o 1970-2099	,-*/

Per visualizzare alcuni esempi, fare clic qui.

6.1.4.5.4 Gestisci sensibilità attivazioni

Per limitare l'esecuzione di un'attività nel caso in cui sia attivata da un evento che si verifica con una certa frequenza, utilizzare la limitazione delle richieste. In determinate circostanze, la limitazione delle richieste può impedire l'esecuzione di un'attivazione. Se viene soddisfatta una qualsiasi delle condizioni definite, le informazioni accumulate per tutti gli osservatori vengono ripristinate (il conteggio riparte da 0). Tali informazioni sono ripristinate anche in caso di riavvio dell'agente o del server ERA. Tutte le modifiche apportate a un'attivazione ne reimpostano lo stato.

Le condizioni di limitazione delle richieste basate sul tempo hanno precedenza rispetto a quelle statistiche. Si consiglia di utilizzare solo una condizione statistica e più condizioni basate sul tempo. La presenza di più condizioni statistiche potrebbe essere inutilmente complessa e alterare i risultati dell'attivazione.

- **Condizioni statistiche**

Le condizioni statistiche possono essere associate con l'operatore logico **E** (devono essere soddisfatte tutte le condizioni) o con l'operatore logico **OPPURE** (la prima condizione soddisfatta attiva l'azione).

- **Condizioni basate sul tempo**

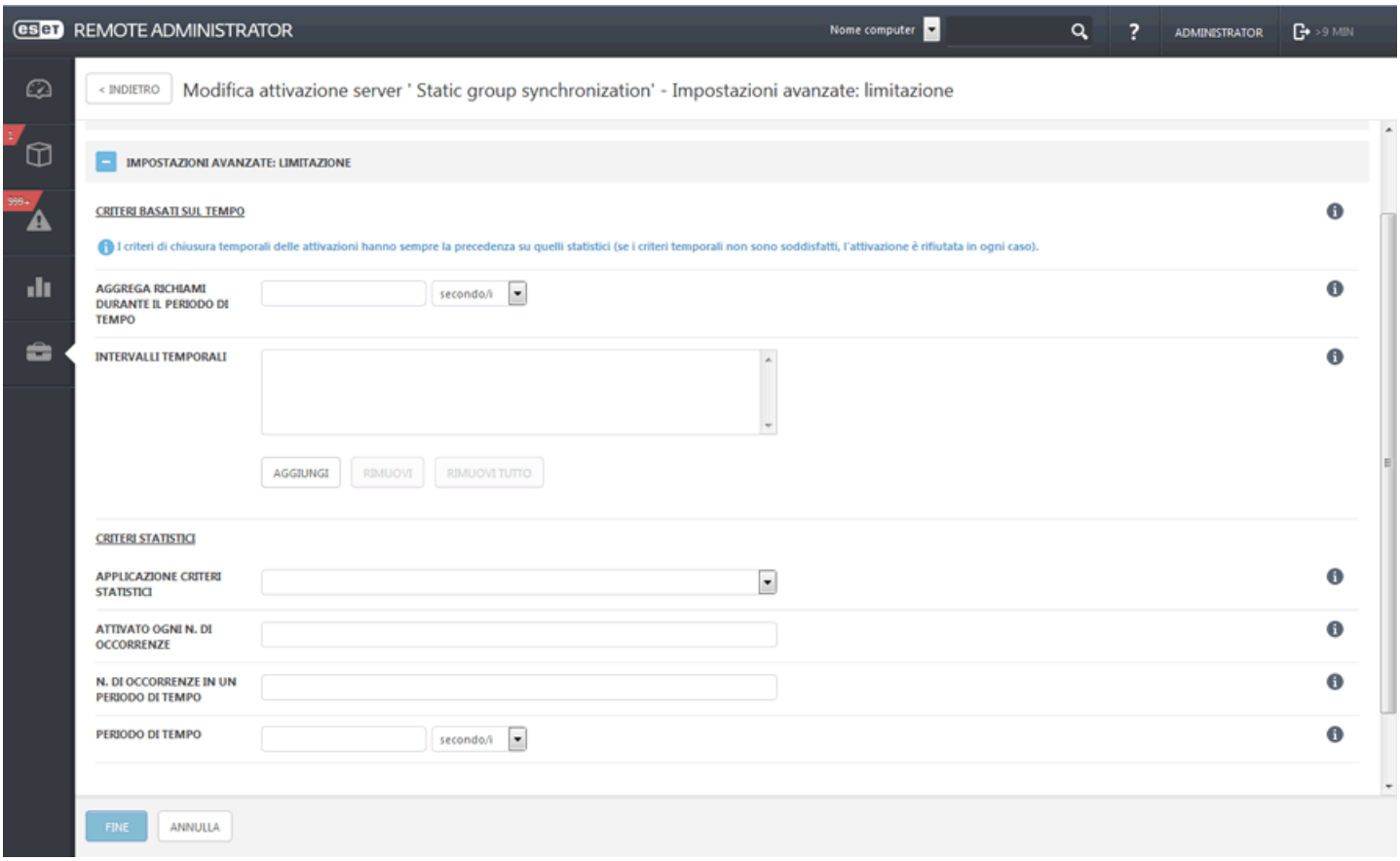
Per poter attivare un evento devono essere soddisfatte tutte le condizioni configurate. I criteri della limitazione delle richieste sono focalizzati sul momento in cui si è verificato l'evento.

Aggregazione

- **Numero di eventi da aggregare**: numero di eventi (quante volte l'attivazione viene eseguita) necessari per eseguire l'attivazione. L'esecuzione dell'attivazione viene impedita fino a quando viene raggiunto questo numero. Ad esempio, se impostato su 100 significa che se vengono rilevate 100 minacce, non si riceveranno 100 notifiche ma una sola notifica contenente 100 minacce. Se vengono rilevate 200 minacce, nella notifica saranno riportate solo le ultime 100 minacce.

Criteri basati sul tempo

- **Aggrega richiami durante il periodo di tempo**: è possibile consentire un risultato ogni X secondi. Se si imposta questa opzione su 10 secondi e in questo intervallo di tempo si verificano 10 richiami, ne sarà conteggiato solo 1.
- **Intervalli temporali**: consente eventi solo nell'intervallo di tempo definito. È possibile aggiungere più intervalli di tempo all'elenco che saranno organizzati in ordine cronologico.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
< INDIETRO
Modifica attivazione server ' Static group synchronization' - Impostazioni avanzate: limitazione
IMPOSTAZIONI AVANZATE: LIMITAZIONE
CRITERI BASATI SUL TEMPO
I criteri di chiusura temporali delle attivazioni hanno sempre la precedenza su quelli statistici (se i criteri temporali non sono soddisfatti, l'attivazione è rifiutata in ogni caso).
AGGREGA RICHIAMI DURANTE IL PERIODO DI TEMPO
secondo/i
INTERVALLI TEMPORALI
AGGIUNGI
RIMUOVI
RIMUOVI TUTTO
CRITERI STATISTICI
APPLICAZIONE CRITERI STATISTICI
ATTIVATO OGNI N. DI OCCORRENZE
N. DI OCCORRENZE IN UN PERIODO DI TEMPO
PERIODO DI TEMPO
secondo/i
FINE
ANNULLA

Criteri statistici

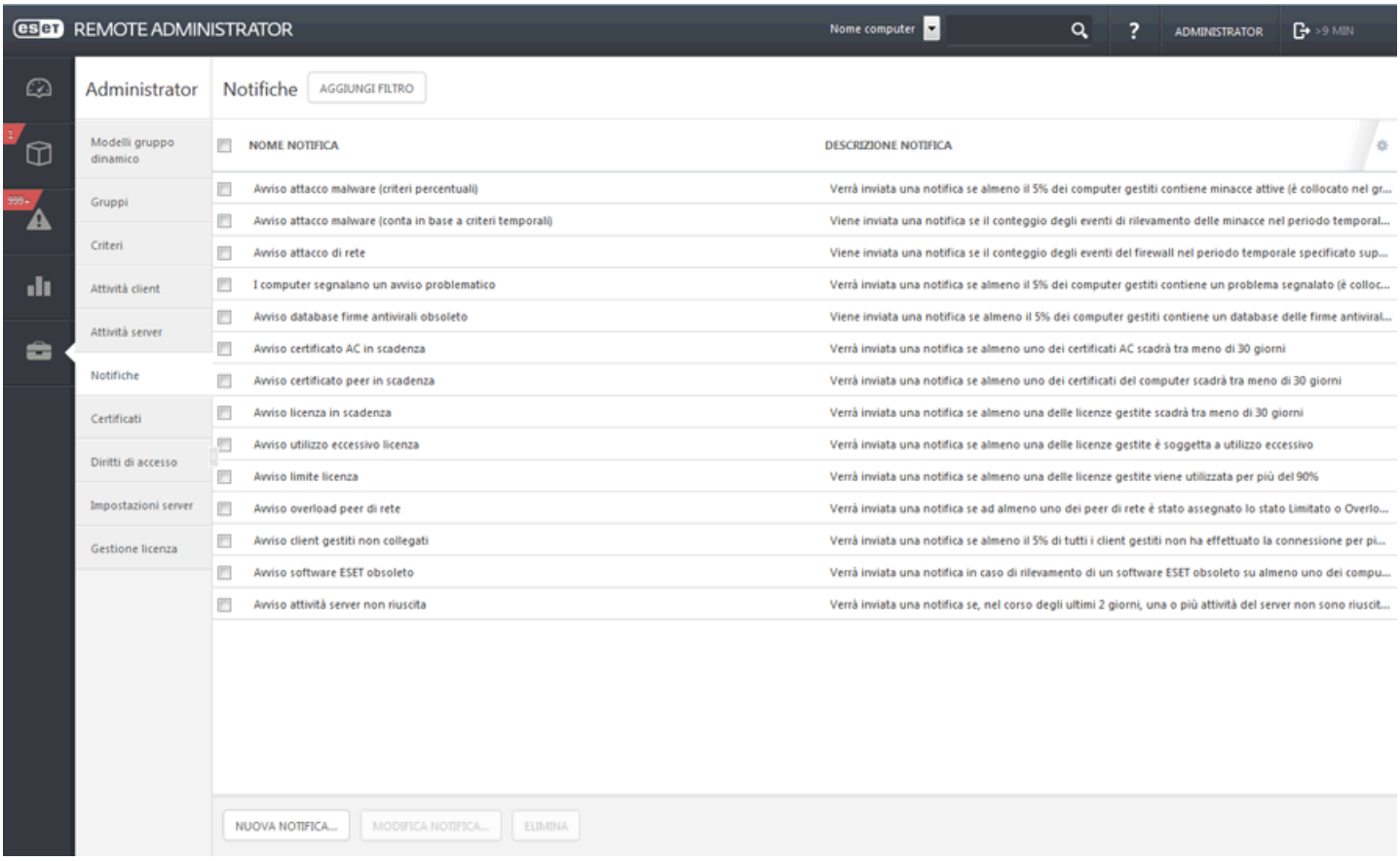
- **Applicazione criteri statistici**: questa opzione consente di definire il metodo in base al quale saranno valutati i criteri statistici. È necessario che siano soddisfatti tutti (**E**), o almeno uno di essi (**OPPURE**).
- **Attivato ogni n. di occorrenze**: consente solo ogni **X** evento (risultato). Ad esempio, se si immette 10, verrà conteggiato solo ciascun 10° evento.
- **N. di occorrenze in un periodo di tempo**: consente solo gli eventi occorsi nel periodo di tempo definito. Definirà la frequenza. Consente ad esempio l'esecuzione dell'attività se l'evento viene rilevato 10 volte in un'ora.
  - **Periodo**: definisce l'intervallo di tempo per l'opzione descritta sopra.
- **Numero di eventi con simbolo**: consente di registrare un evento (risultato) se si verificano **X** eventi con il simbolo specifico. Ad esempio, se si immette 10, per la decima installazione di una determinata applicazione verrà conteggiato un evento.
  - **Applica se il numero di eventi**: immettere un numero di eventi consecutivi dall'ultimo evento per conteggiare un altro evento. Ad esempio immettere 10 per conteggiare un evento dopo 10 eventi dall'ultimo evento.

- **Applica se il numero di eventi**: l'attivazione viene applicata quando l'evento viene **Ricevuto in una riga** (l'esecuzione dell'attivazione non viene considerata) o **Ricevuto sin dall'esecuzione dell'ultima attivazione** (all'esecuzione dell'attivazione, il numero viene ripristinato su 0).

6.1.5 Notifiche

Le **Notifiche** sono essenziali per tenere traccia dello stato complessivo della rete. Quando si verifica un nuovo evento (in base alla configurazione), l'utente riceverà una notifica tramite un metodo definito (un trap SNMP o un messaggio e-mail) al quale è possibile rispondere di conseguenza.

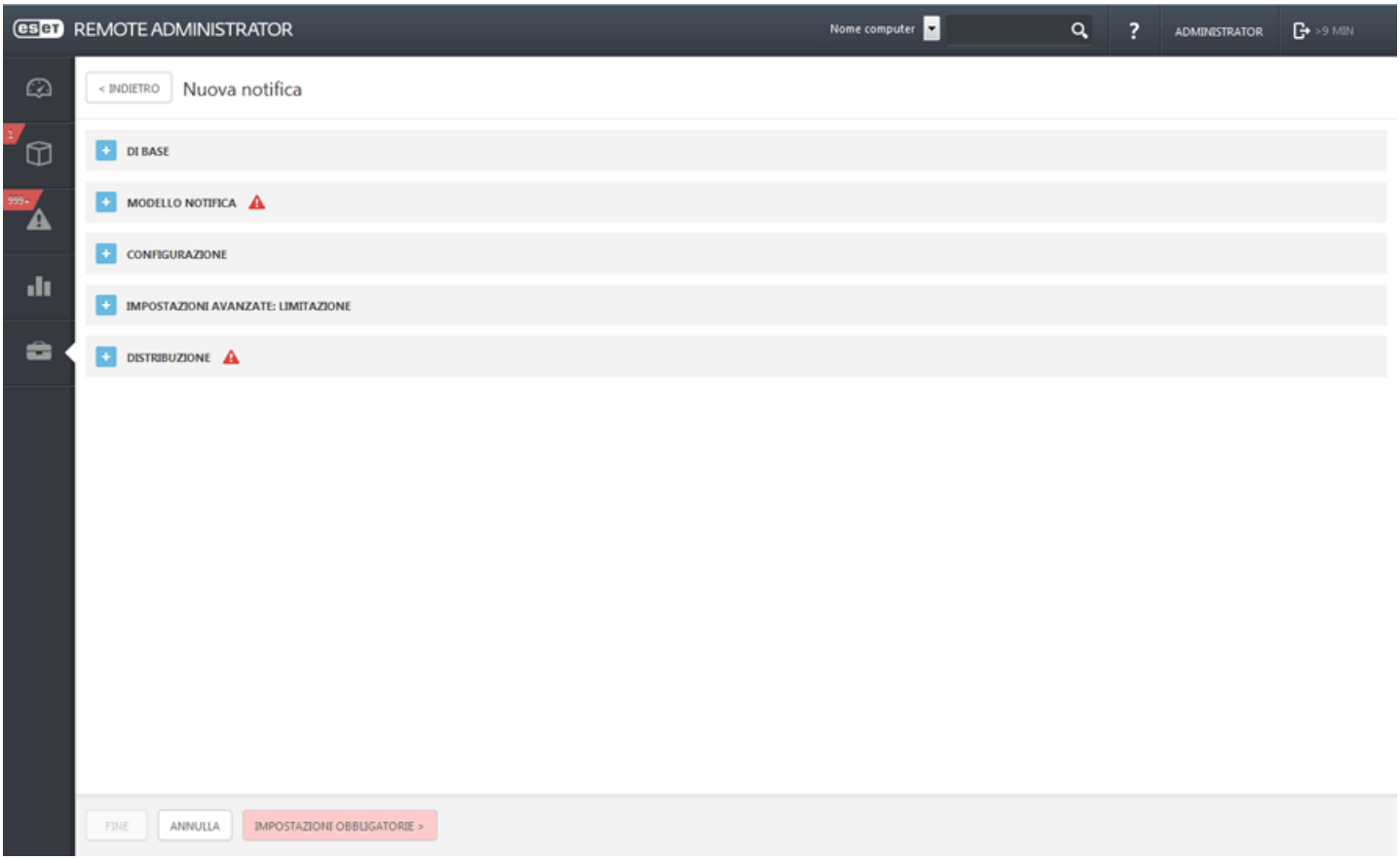
- Nell'elenco sono visualizzati tutti i modelli di notifiche ed è possibile filtrarli in base al **Nome** o alla **Descrizione**.
- Fare clic su **Aggiungi filtro** per aggiungere i criteri di filtraggio e/o immettere una stringa nel campo **Nome**/ **Notifica**.
- Se si seleziona una notifica esistente è possibile **Modificarla** o **Eliminarla** completamente.
- Per creare una nuova notifica fare su Nuova notifica nella parte inferiore della pagina.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Notifiche
AGGIUNGI FILTRO
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
NOME NOTIFICA
DESCRIZIONE NOTIFICA
Avviso attacco malware (criteri percentuali)
Verrà inviata una notifica se almeno il 5% dei computer gestiti contiene minacce attive (è collocato nel gr...
Avviso attacco malware (conta in base a criteri temporali)
Viene inviata una notifica se il conteggio degli eventi di rilevamento delle minacce nel periodo temporal...
Avviso attacco di rete
Viene inviata una notifica se il conteggio degli eventi del firewall nel periodo temporale specificato sup...
I computer segnalano un avviso problematico
Verrà inviata una notifica se almeno il 5% dei computer gestiti contiene un problema segnalato (è colloc...
Avviso database firme antivirali obsoleto
Viene inviata una notifica se almeno il 5% dei computer gestiti contiene un database delle firme antiviral...
Avviso certificato AC in scadenza
Verrà inviata una notifica se almeno uno dei certificati AC scadrà tra meno di 30 giorni
Avviso certificato peer in scadenza
Verrà inviata una notifica se almeno uno dei certificati del computer scadrà tra meno di 30 giorni
Avviso licenza in scadenza
Verrà inviata una notifica se almeno una delle licenze gestite scadrà tra meno di 30 giorni
Avviso utilizzo eccessivo licenza
Verrà inviata una notifica se almeno una delle licenze gestite è soggetta a utilizzo eccessivo
Avviso limite licenza
Verrà inviata una notifica se almeno una delle licenze gestite viene utilizzata per più del 90%
Avviso overload peer di rete
Verrà inviata una notifica se ad almeno uno dei peer di rete è stato assegnato lo stato Limitato o Overlo...
Avviso client gestiti non collegati
Verrà inviata una notifica se almeno il 5% di tutti i client gestiti non ha effettuato la connessione per pi...
Avviso software ESET obsoleto
Verrà inviata una notifica in caso di rilevamento di un software ESET obsoleto su almeno uno dei compu...
Avviso attività server non riuscita
Verrà inviata una notifica se, nel corso degli ultimi 2 giorni, una o più attività del server non sono riuscit...
NUOVA NOTIFICA...
MODIFICA NOTIFICA...
ELIMINA

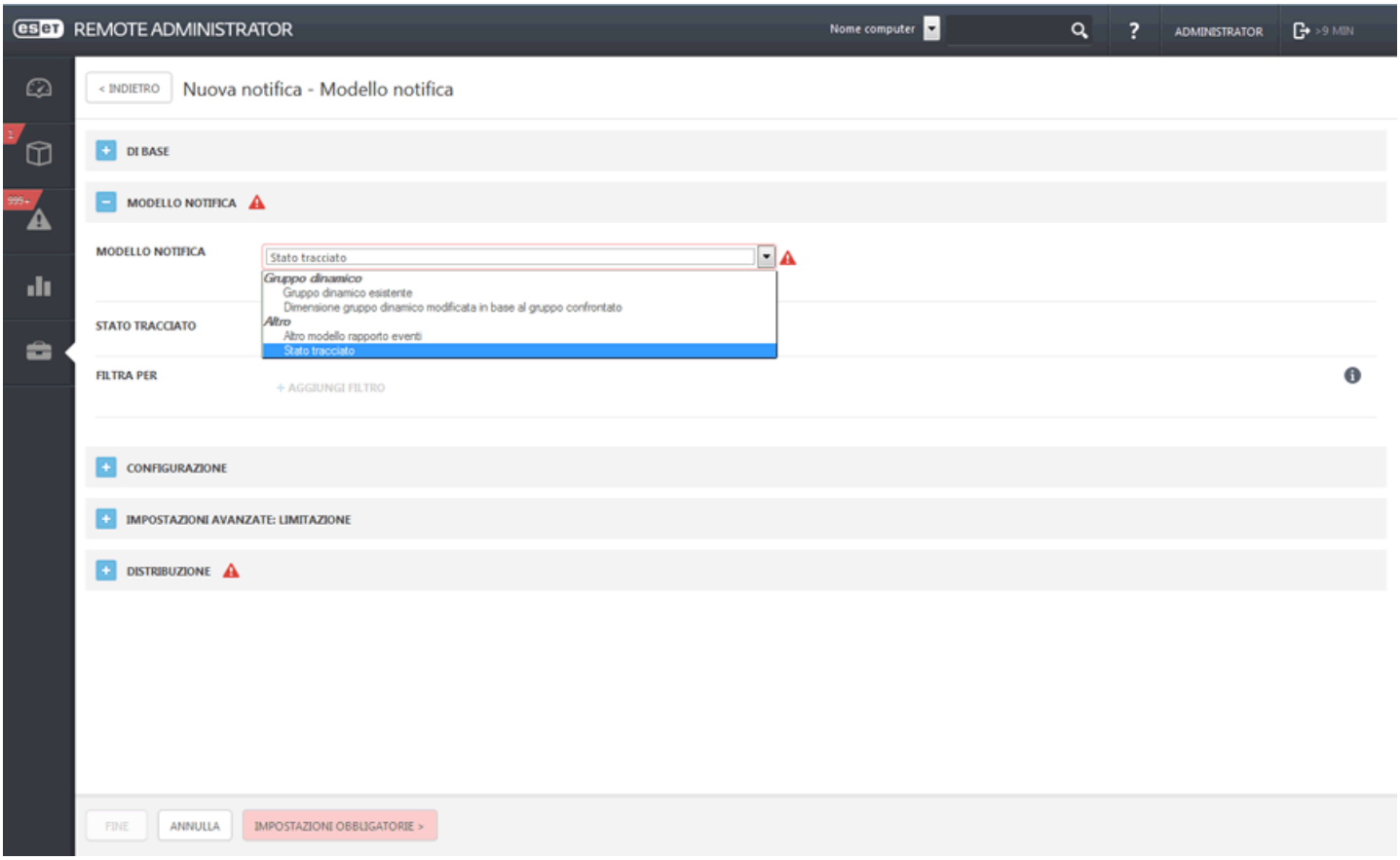
6.1.5.1 Procedura guidata notifiche

Di base

Contiene il **Nome** e la **Descrizione** della notifica. Si tratta di informazioni importanti per filtrare più notifiche. Il filtro si trova nella parte superiore della pagina **Notifica**.



Modello notifica



Gruppo dinamico esistente: un gruppo dinamico esistente verrà utilizzato per generare le notifiche. Selezionare un Gruppo dinamico dall'elenco e fare clic su **OK**.
Dimensione gruppo dinamico modificata in base al gruppo confrontato: se il numero dei client in un Gruppo dinamico osservato viene modificato rispetto a un gruppo messo a confronto (statico o dinamico), verrà invocata la notifica.**Altro modello rapporto eventi:** utilizzare questa opzione per le notifiche non associate a un Gruppo dinamico ma basate su eventi di sistema filtrati dal rapporto eventi. Selezionare un **Tipo di rapporto** sul quale si baserà la notifica e un **Operatore logico** per i filtri.

Stato tracciato: questa opzione consente di ricevere notifiche relative ai cambiamenti di stato dell'oggetto utilizzando i filtri definiti dall'utente.

Configurazione

Notifica ogni volta che il contenuto del gruppo dinamico cambia: l'attivazione di questa opzione consente di ricevere notifiche quando i membri in un Gruppo dinamico vengono aggiunti, rimossi o modificati.
Periodo temporale notifica: consente di definire l'intervallo di tempo (in minuti, ore o giorni) per il confronto con il nuovo stato. Ad esempio, 7 giorni fa il numero di client con prodotti di protezione obsoleti era 10 e la **Soglia** (vedere di seguito) era impostata su 20. Se il numero di client con un prodotto di protezione obsoleto diventa 30, l'utente riceverà una notifica.

Soglia: consente di definire una soglia che attiverà l'invio di una notifica. È possibile definire un numero o una percentuale di client (membri di un Gruppo dinamico).
Messaggio generato: messaggio predefinito che apparirà nella notifica. Contiene le impostazioni configurate in formato testo.
Messaggio: oltre al messaggio predefinito è possibile aggiungerne uno personalizzato che apparirà alla fine del precedente messaggio predefinito. Si tratta di un'opzione facoltativa ma è consigliata per filtrare al meglio le notifiche.

NOTA: le opzioni di configurazione possono differenziarsi rispetto ai differenti modelli di notifica.

Impostazioni avanzate: limitazione delle richieste

Criteri basati sul tempo

- Specificare il **Numero di eventi da aggregare**. Questa opzione consente di definire il numero di eventi (risultati eventi) necessari per attivare l'invio della notifica. Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Criteri statistici

- **Applicazione criteri statistici**: questa opzione consente di definire il metodo in base al quale saranno valutati i criteri statistici. È necessario che siano soddisfatti tutti (**E**), o almeno uno di essi (**OPPURE**).
- **Attivato ogni n. di occorrenze**: consente solo ogni **X** evento (risultato). Ad esempio, se si immette 10, verrà conteggiato solo ciascun 10° evento.
- **N. di occorrenze in un periodo di tempo**: consente solo gli eventi occorsi nel periodo di tempo definito. Definirà la frequenza. Consente ad esempio l'esecuzione dell'attività se l'evento viene rilevato 10 volte in un'ora. **Periodo**: definisce l'intervallo di tempo per l'opzione descritta sopra.
- **Numero di eventi con simbolo**: consente un evento (risultato) se si verificano **X** eventi con il simbolo specifico. Ad esempio, se si immette 10, per 10 installazioni di un determinato software verrà conteggiato un evento. **Applica se il numero di eventi**: immettere un numero di eventi consecutivi dall'ultimo evento per conteggiare un altro evento. Ad esempio, immettere 10 per conteggiare un evento dopo 10 eventi dall'ultimo evento.
- **Applica se il numero di eventi**: l'attivazione viene applicata quando l'evento viene **Ricevuto in una riga** (l'esecuzione dell'attivazione non viene considerata) o **Ricevuto sin dall'esecuzione dell'ultima attivazione** (all'esecuzione dell'attivazione, il numero viene ripristinato su 0).

➖ Distribuzione

Oggetto: oggetto del messaggio contenente la notifica. Si tratta di un'opzione facoltativa ma è consigliata per un miglior filtraggio o quando si creano regole per ordinare i messaggi di notifica.

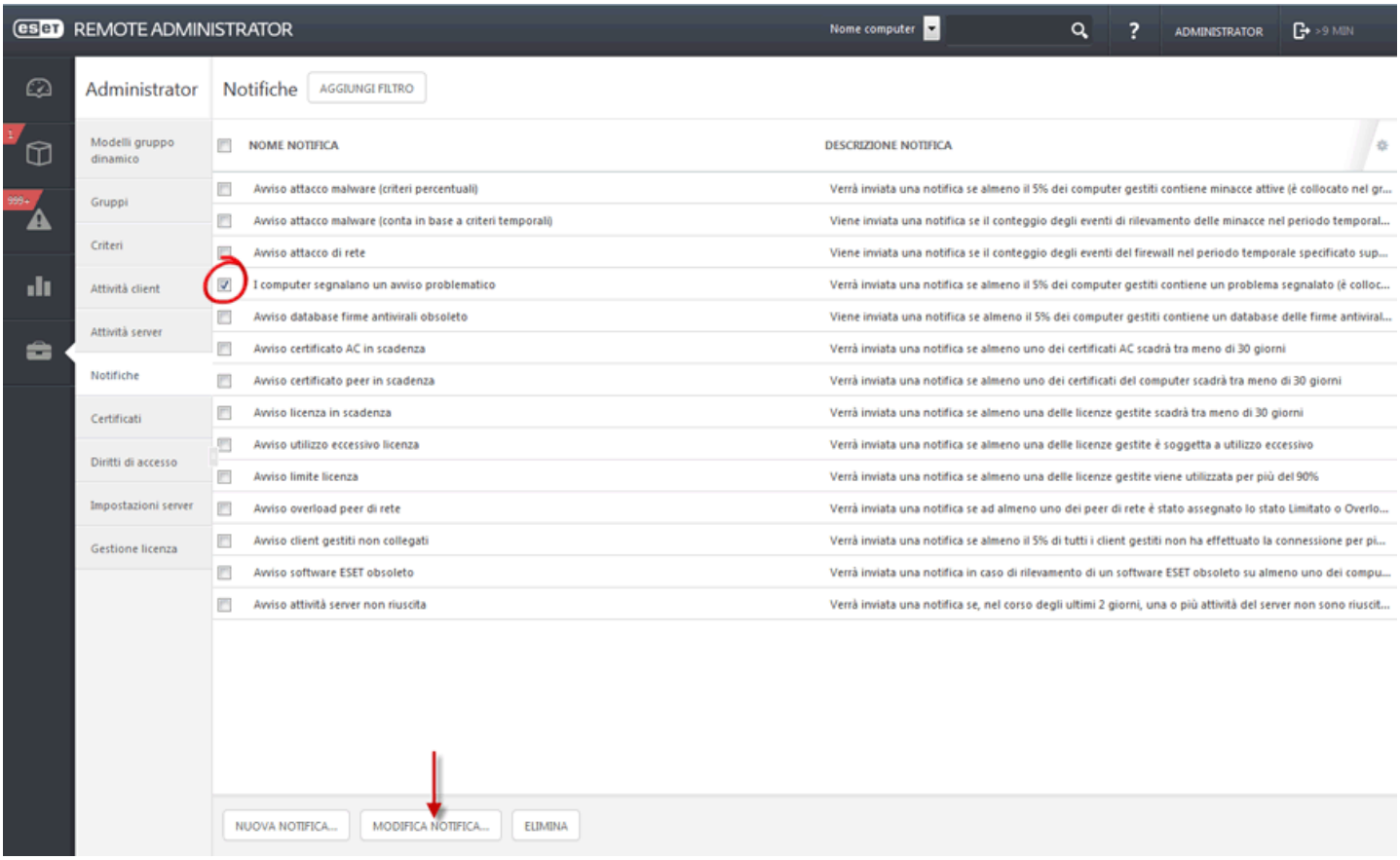
Distribuzione

- **Invia trap SNMP**: consente di inviare un trap SNMP. Il trap SNMP notifica il server tramite un messaggio SNMP non richiesto. Per ulteriori informazioni, consultare il capitolo Come configurare un servizio trap SNMP.
- **Invia e-mail**: consente l'invio di un messaggio e-mail basato sulle impostazioni di posta elettronica.

Indirizzi e-mail: immettere gli indirizzi e-mail dei destinatari dei messaggi di notifica, separando più indirizzi con una virgola (",").

6.1.5.2 Gestisci notifiche

Le notifiche sono gestite nella scheda Amministrazione. Selezionare una notifica e fare clic su Modifica notifica.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Notifiche
AGGIUNGI FILTRO
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
NOME NOTIFICA
DESCRIZIONE NOTIFICA
Avviso attacco malware (criteri percentuali)
Verrà inviata una notifica se almeno il 5% dei computer gestiti contiene minacce attive (è collocato nel gr...
Avviso attacco malware (conta in base a criteri temporali)
Viene inviata una notifica se il conteggio degli eventi di rilevamento delle minacce nel periodo temporal...
Avviso attacco di rete
Viene inviata una notifica se il conteggio degli eventi del firewall nel periodo temporale specificato sup...
I computer segnalano un avviso problematico
Verrà inviata una notifica se almeno il 5% dei computer gestiti contiene un problema segnalato (è colloc...
Avviso database firme antivirali obsoleto
Viene inviata una notifica se almeno il 5% dei computer gestiti contiene un database delle firme antiviral...
Avviso certificato AC in scadenza
Verrà inviata una notifica se almeno uno dei certificati AC scadrà tra meno di 30 giorni
Avviso certificato peer in scadenza
Verrà inviata una notifica se almeno uno dei certificati del computer scadrà tra meno di 30 giorni
Avviso licenza in scadenza
Verrà inviata una notifica se almeno una delle licenze gestite scadrà tra meno di 30 giorni
Avviso utilizzo eccessivo licenza
Verrà inviata una notifica se almeno una delle licenze gestite è soggetta a utilizzo eccessivo
Avviso limite licenza
Verrà inviata una notifica se almeno una delle licenze gestite viene utilizzata per più del 90%
Avviso overload peer di rete
Verrà inviata una notifica se ad almeno uno dei peer di rete è stato assegnato lo stato Limitato o Overlo...
Avviso client gestiti non collegati
Verrà inviata una notifica se almeno il 5% di tutti i client gestiti non ha effettuato la connessione per pi...
Avviso software ESET obsoleto
Verrà inviata una notifica in caso di rilevamento di un software ESET obsoleto su almeno uno dei compu...
Avviso attività server non riuscita
Verrà inviata una notifica se, nel corso degli ultimi 2 giorni, una o più attività del server non sono riuscit...
NUOVA NOTIFICA...
MODIFICA NOTIFICA...
ELIMINA

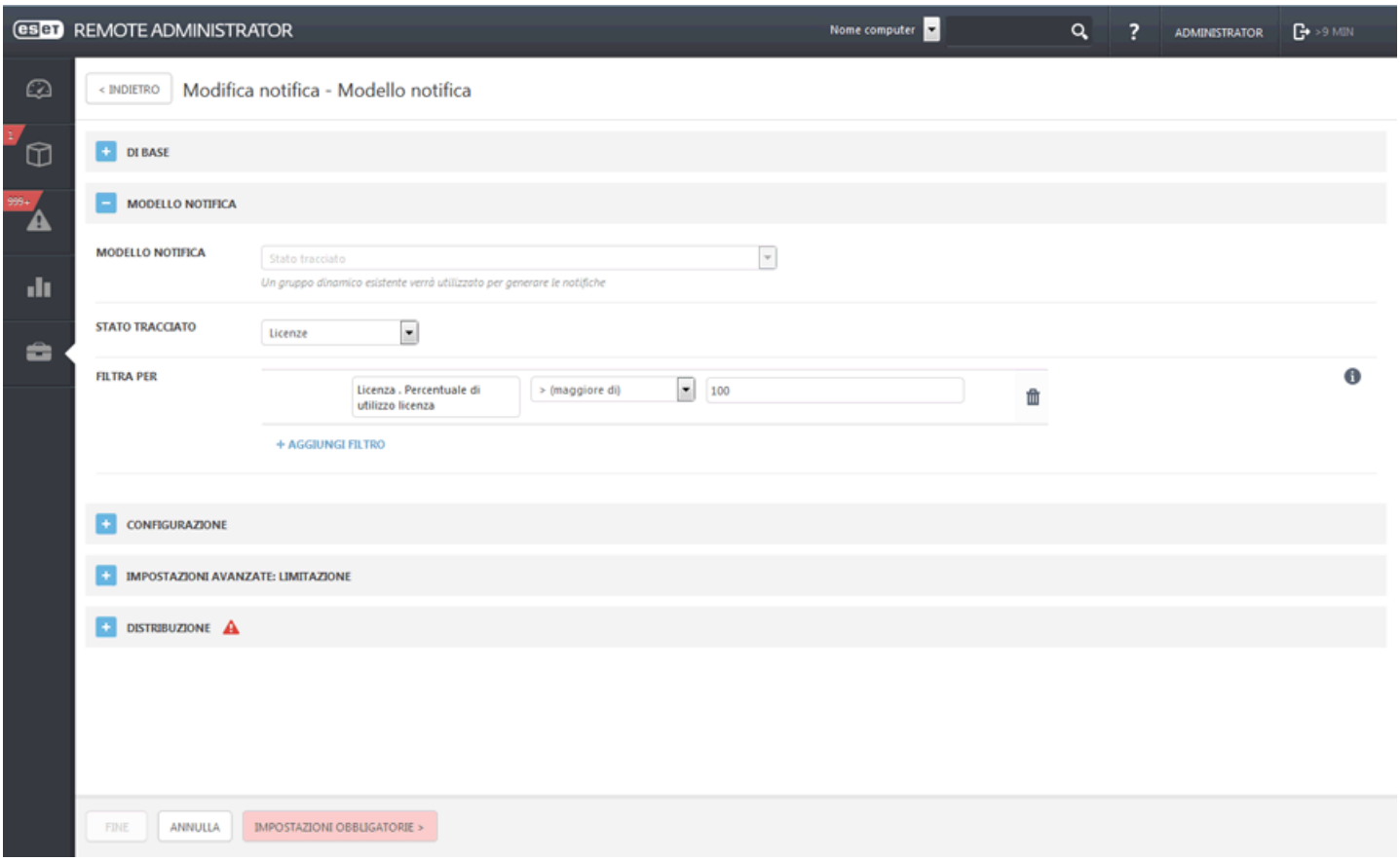
Di base

È possibile modificare il **Nome notifica** e la **Descrizione**. È importante per filtrare più notifiche.

Modello notifica

Gruppo dinamico esistente: un gruppo dinamico esistente verrà utilizzato per generare le notifiche. Selezionare un Gruppo dinamico dall'elenco e fare clic su **OK**.
Dimensione gruppo dinamico modificata in base al gruppo confrontato: se il numero dei client in un Gruppo dinamico osservato viene modificato rispetto a un gruppo messo a confronto (statico o dinamico), verrà invocata la notifica.
Altro modello rapporto eventi
utilizzare questa opzione per le notifiche non associate a un Gruppo dinamico ma basate su eventi di sistema filtrati dal rapporto eventi. Selezionare un **Tipo di rapporto** sul quale si baserà la notifica e un **Operatore logico** per i filtri.
Stato tracciato: questa opzione consente di ricevere notifiche relative ai cambiamenti di stato dell'oggetto utilizzando i filtri definiti dall'utente.

NOTA: è possibile modificare lo Stato tracciato e utilizzare le opzioni **+ Aggiungi filtro** oppure **Operatore logico** per i filtri.



Configurazione

Notifica ogni volta che il contenuto del gruppo dinamico cambia: l'attivazione di questa opzione consente di ricevere notifiche quando i membri in un Gruppo dinamico vengono aggiunti, rimossi o modificati.
Periodo temporale notifica: consente di definire l'intervallo di tempo (in minuti, ore o giorni) per il confronto con il nuovo stato. Ad esempio, 7 giorni fa il numero di client con prodotti di protezione obsoleti era 10 e la **Soglia** (vedere di seguito) era impostata su 20. Se il numero di client con un prodotto di protezione obsoleto diventa 30, l'utente riceverà una notifica.
Soglia: consente di definire una soglia che attiverà l'invio di una notifica. È possibile definire un numero o una percentuale di client (membri del Gruppo dinamico).
Messaggio generato: messaggio predefinito che apparirà nella notifica. Contiene le impostazioni configurate in formato testo.
Messaggio: oltre al messaggio predefinito è possibile aggiungerne uno personalizzato che apparirà alla fine del precedente messaggio predefinito. Si tratta di un'opzione facoltativa ma è consigliata per filtrare al meglio le notifiche e la panoramica.

NOTA: le opzioni disponibili dipendono dal modello di notifica selezionato.

Impostazioni avanzate: limitazione delle richieste

Criteri basati sul tempo

- Specificare il **Numero di eventi da aggregare**. Questa opzione consente di definire il numero di eventi (risultati eventi) necessari per attivare l'invio della notifica. Per ulteriori informazioni, consultare il capitolo Limitazione delle richieste.

Criteri statistici

- **Applicazione criteri statistici**: questa opzione consente di definire il metodo in base al quale saranno valutati i criteri statistici. È necessario che siano soddisfatti tutti (**E**), o almeno uno di essi (**OPPURE**).
- **Attivato ogni n. di occorrenze**: consente solo ogni **X** evento (risultato). Ad esempio, se si immette 10, verrà conteggiato solo ciascun 10° evento.
- **N. di occorrenze in un periodo di tempo**: consente solo gli eventi occorsi nel periodo di tempo definito. Definirà la frequenza. Consente ad esempio l'esecuzione dell'attività se l'evento viene rilevato 10 volte in un'ora. **Periodo**: definisce l'intervallo di tempo per l'opzione descritta sopra.
- **Numero di eventi con simbolo**: consente un evento (risultato) se si verificano **X** eventi con il simbolo specifico. Ad esempio, se si immette 10, per 10 installazioni di un determinato software verrà conteggiato un evento. **Applica se il numero di eventi**: immettere un numero di eventi consecutivi dall'ultimo evento per conteggiare un altro evento. Ad esempio, immettere 10 per conteggiare un evento dopo 10 eventi dall'ultimo evento.
- **Applica se il numero di eventi**: l'attivazione viene applicata quando l'evento viene **Ricevuto in una riga** (l'esecuzione dell'attivazione non viene considerata) o **Ricevuto sin dall'esecuzione dell'ultima attivazione** (all'esecuzione dell'attivazione, il numero viene ripristinato su 0).

Distribuzione

Oggetto: oggetto del messaggio contenente la notifica. Si tratta di un'opzione facoltativa ma è consigliata per un miglior filtraggio o quando si creano regole per ordinare i messaggi.

Distribuzione

- **Invia trap SNMP**: consente di inviare un trap SNMP. Il trap SNMP notifica il server tramite un messaggio SNMP non richiesto. Per ulteriori informazioni, consultare il capitolo Come configurare un servizio trap SNMP.
- **Invia e-mail**: consente l'invio di un messaggio e-mail basato sulle impostazioni di posta elettronica.

Indirizzi e-mail: immettere gli indirizzi e-mail dei destinatari dei messaggi di notifica, separando più indirizzi con una virgola (",").

6.1.5.3 Come configurare un servizio trap SNMP

Per ricevere correttamente messaggi SNMP, è necessario che sia configurato il servizio trap SNMP.

Passaggi di configurazione in base al sistema operativo

- Windows
- Linux

WINDOWS

Prerequisiti

- È necessario che il servizio **Simple Network Management Protocol** sia installato sulla macchina in cui è installato il server ERA, oltre alla macchina sulla quale sarà installato il software trap SNMP.
- Entrambi i (precedenti) computer devono trovarsi nella stessa subnet.
- Il servizio SNMP deve essere configurato sul computer del server ERA.

Configurazione del servizio SNMP (server ERA)

- Premere il tasto Windows + R per aprire una finestra di dialogo di esecuzione, immettere *Services.msc* nel campo **Apri** e premere **Invio**. Ricercare il servizio SNMP.
- Aprire la scheda **Trap**, immettere **pubblico** nel campo **Nome community** e fare clic su **Aggiungi a elenco**.
- Fare clic su **Aggiungi,** immettere il **Nome host, indirizzo IP** o **IPX** del computer dove è installato il software di trapping SNMP nel campo appropriato e fare clic su **Aggiungi**.
- Andare alla scheda **Protezione**. Fare clic su **Aggiungi** per visualizzare la finestra **Configurazione del servizio SNMP**. Immettere **pubblico** nel campo **Nome community** e fare clic su **Aggiungi**. I diritti saranno impostati su **DI SOLA LETTURA**. Lasciare questa impostazione invariata.
- Assicurarsi che l'opzione **Accetta pacchetti SNMP da questi host** sia selezionata e fare clic su **OK** per confermare. Il servizio SNMP non è configurato.

Configurazione software trap SNMP (client)

- Il servizio SNMP è installato e non è necessario configurarlo.
- Installare **AdRem SNMP Manager** o **AdRem NetCrunch**.
- **AdRem SNMP Manager**: avviare l'applicazione e selezionare **Crea nuovo elenco nodi SNMP.** Fare clic su **Sì** per confermare.
- Controllare l'indirizzo di rete della subnet (visualizzato in questa finestra). Fare clic su **OK** per eseguire una ricerca nella rete.
- Attendere il termine della ricerca, i cui risultati saranno visualizzati nella finestra **Risultati individuazione**. L'indirizzo IP del server ERA è visualizzato in questo elenco.
- Selezionare l'indirizzo IP del server e fare clic su **OK**. L'indirizzo del server è visualizzato nella sezione **Nodi**.
- Fare clic su **Ricevente trap interrotto** e selezionare **Avvia**. Verrà visualizzato **Ricevente trap avviato**. Ora è possibile ricevere messaggi SNMP dal server ERA.

LINUX

1. Installare il pacchetto snmpd eseguendo uno dei seguenti comandi:
   `apt-get install snmpd snmp` (Distribuzioni Debian, Ubuntu)
   `yum install net-snmp` (Distribuzioni Red-Hat, Fedora)

2. Aprire il file */etc/default/snmpd* e apportare le seguenti modifiche agli attributi:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```
Se si aggiunge # , la riga verrà completamente disabilitata.

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
```
Aggiungere questa riga al file.

```
TRAPDRUN=yes
```
Modificare l'attributo *trapdrun* su *yes*.

3. Creare un backup del file *snmpd.conf* originale. Il file verrà modificato più avanti.

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. Creare un nuovo file *snmpd.conf* e aggiungere le righe seguenti:

```
rocommunity public
syslocation "Testing ERA6"
syscontact admin@ERA6.com
```

5. Aprire il file */etc/snmp/snmptrapd.conf* e aggiungere la seguente riga alla fine del file:

```
authCommunity log,execute,net public
```

6. Immettere il seguente comando per avviare i servizi del gestore SNMP e la registrazione dei trap in ingresso:

```
/etc/init.d/snmpd restart
```
oppure
```
service snmpd restart
```

7. Per controllare il corretto funzionamento del trap e la ricezione dei messaggi, eseguire il seguente comando:

```
tail -f /var/log/syslog | grep -i TRAP
```

6.1.6 Certificati

Un certificato autentica i dati scambiati nelle comunicazioni tra il server ERA e l'agente poiché il server ERA comunica anche tramite un agente.

- Crea un nuovo certificato tramite l'autorità di certificazione ERA
- Crea un nuovo certificato tramite un'autorità di certificazione personalizzata
- Crea una nuova autorità di certificazione

6.1.6.1 Certificati del peer

Un certificato autentica i dati nelle comunicazioni tra il server ERA e l'agente poiché il server ERA comunica anche tramite un agente.

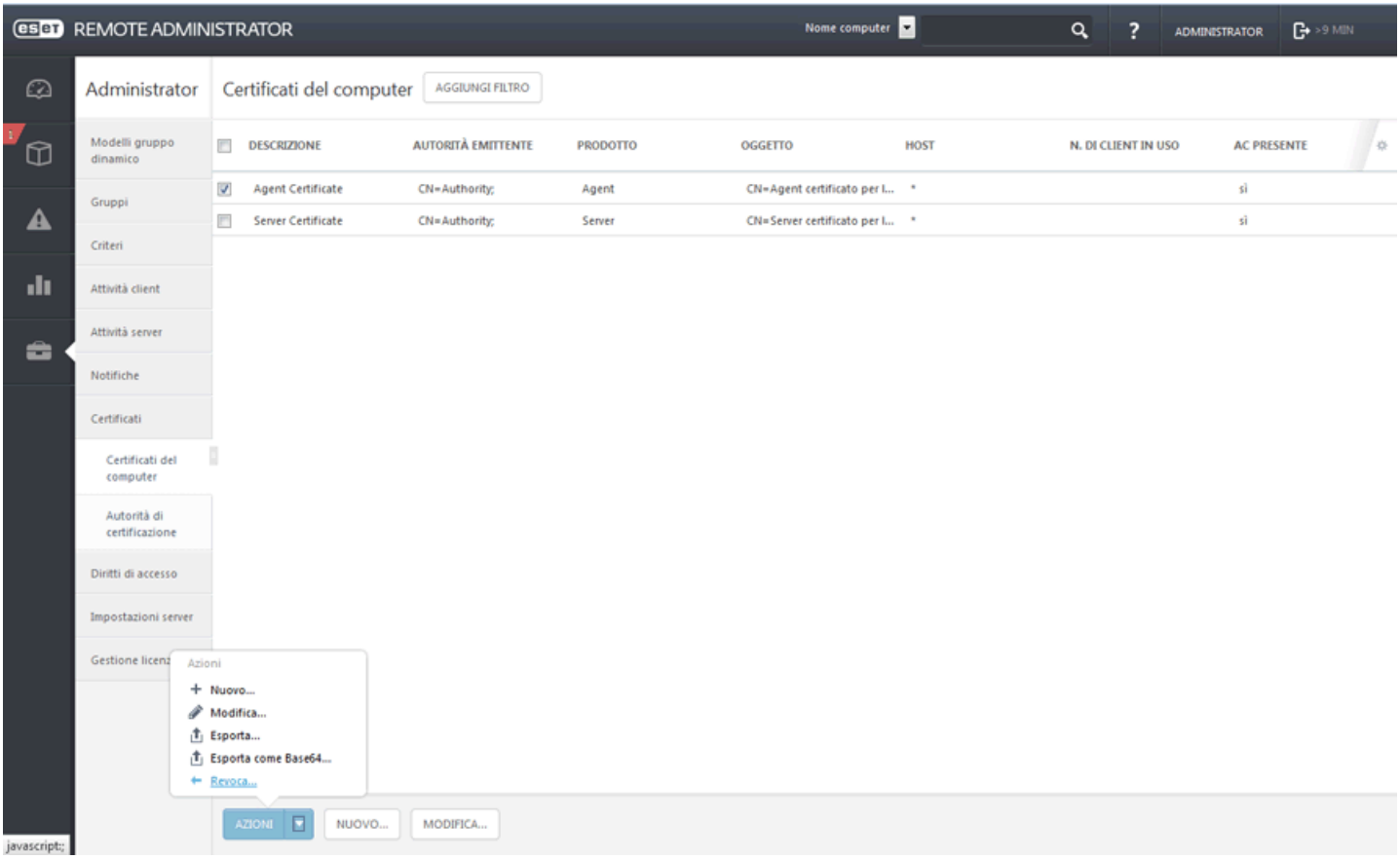
+ Nuovo... - questa opzione consente di accedere alle attività crea un nuovo certificato tramite l'autorità di certificazione ERA o crea un nuovo certificato tramite un'autorità di certificazione personalizzata. Questi certificati sono utilizzati per l'Agente, il Proxy e il Server.

Modifica...: selezionare questa opzione per modificare un certificato esistente dall'elenco. Le stesse opzioni sono applicabili quando si crea un nuovo certificato.

Esporta...: usare questa opzione per esportare il certificato come un file. Questo file è necessario se si installa l'agente a livello locale su un computer o quando si installa la funzionalità Connettore dispositivi mobili.

Esporta come Base64...: usare questa opzione per esportare il certificato come un file .txt.

Revoca...: se non si desidera più utilizzare il certificato, selezionare Revoca. Questa opzione invalida il certificato. I certificati non validi non saranno accettati da ESET Remote Administrator.

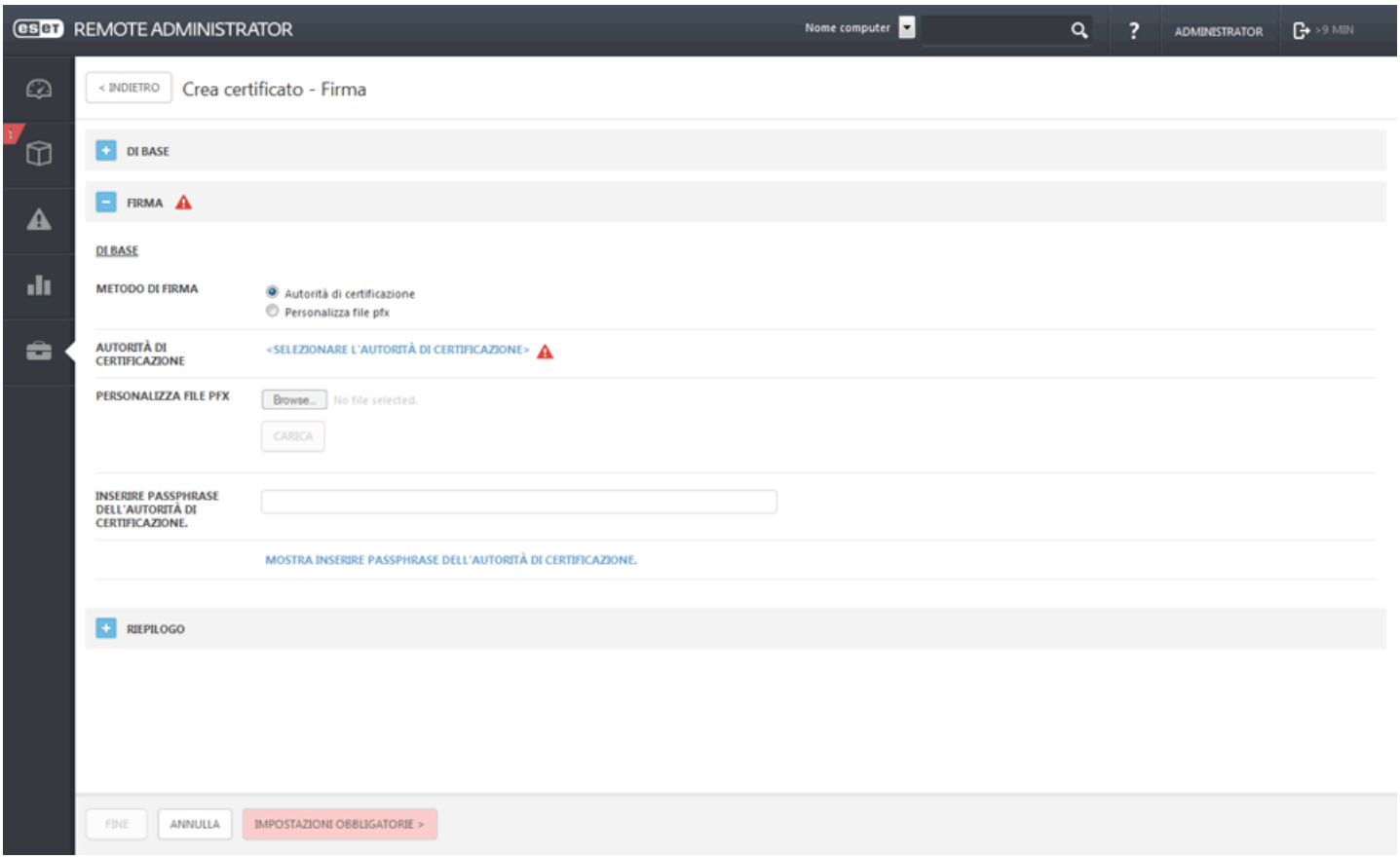


6.1.6.1.1 Crea un nuovo certificato tramite l'autorità di certificazione ERA

Per creare una nuova autorità in **ERA Web Console**, accedere ad **Amministrazione** > **Certificati** e fare clic su **Azioni** > **Nuova**.

Di base

- Immettere una **Descrizione** per il certificato e selezionare **Agente** come **Prodotto**.
- Immettere una connessione al server ERA nel campo **Host**. Può essere un nome host, un indirizzo IP o un nome parziale con un carattere jolly ("*"). Immettere più voci separandole con uno spazio (" "), virgola (",") o punto e virgola (";").
- Immettere una password nei campi **Passphrase** e di conferma. Questa password verrà utilizzata durante l'installazione dell'agente.
- Immettere un valore nel campo **Nome comune**. Questo valore dovrebbe contenere la stringa "Agente", "Proxy" o "Server" a seconda del **Prodotto** selezionato.
- Facoltativamente, è possibile inserire una descrizione sul certificato.
- Immettere i valori **Valido da** e **Valore su** per assicurare che il certificato sia valido.



Firma

- Il metodo di firma dovrebbe essere l'**Autorità di certificazione**.
- Selezionare l'**Autorità di certificazione ERA** creata durante l'installazione iniziale.
- Saltare l'opzione relativa al `file pfx` personalizzato, in quanto è applicabile esclusivamente alle autorità di certificazione `pfx` auto-firmate.
- Immettere la password per il certificato: è la **Passphrase autorità di certificazione** creata durante l'installazione del server.

Riepilogo

- Rivedere le informazioni sul certificato immesse e fare clic su **Fine**. Il certificato è stato creato correttamente e sarà disponibile nell'elenco **Certificati** per poter essere utilizzato durante l'installazione dell'agente.

6.1.6.1.2 Crea un nuovo certificato tramite un'autorità di certificazione personalizzata

Per creare una nuova autorità in **ERA Web Console**, accedere ad **Amministrazione** > **Certificati** e fare clic su **Azioni** > **Nuova**.

Di base

- Immettere una **Descrizione** per il certificato e selezionare **Agente** come **Prodotto**.
- Immettere una connessione al server ERA nel campo **Host**. Può essere un nome host, un indirizzo IP o un nome parziale con un carattere jolly ("*"). Immettere più voci separandole con uno spazio (" "), virgola (",") o punto e virgola (";").
- Immettere una password nei campi **Passphrase** e di conferma. Questa password verrà utilizzata durante l'installazione dell'agente.
- Immettere un valore nel campo **Nome comune**. Questo valore dovrebbe contenere la stringa "Agente", "Proxy" o "Server" a seconda del **Prodotto** selezionato.
- Facoltativamente, è possibile inserire una descrizione sul certificato.
- Immettere i valori **Valido da** e **Valore su** per assicurare che il certificato sia valido.

Firma

- Il metodo di firma dovrebbe essere **Personalizza file pfx**.
- Fare clic su **Sfoglia** per selezionare un `file pfx` personalizzato. Accedere al `file pfx` personalizzato e fare clic su **OK**. Fare clic su **Carica** per caricare questo certificato sul server.
- Immettere la password per il certificato: è la **Passphrase autorità di certificazione** creata durante l'installazione del server.

Riepilogo

- Rivedere le informazioni sul certificato immesse e fare clic su **Fine**. Il certificato è stato creato correttamente e può essere utilizzato per installare l'agente.

6.1.6.2 Autorità di certificazione

Nella sezione **Autorità di certificazione** sono elencate e gestite le Autorità di certificazione. Se si utilizzano più Autorità di certificazione, potrebbe essere utile applicare un filtro per ordinarle.

Fare clic su **Aggiungi filtro** nella parte superiore della pagina e selezionare i criteri di filtraggio che si desiderano utilizzare (Descrizione, Oggetto, Valido da/fino a, ecc.). È possibile impostare un criterio per filtro. Dopo aver selezionato un criterio e aver fatto clic su OK, accanto al pulsante Aggiungi filtro verrà visualizzato un campo di testo. In questo campo è possibile immettere informazioni personalizzate, ad esempio una **Data** e una **Descrizione**. Per creare altri filtri, fare clic su Aggiungi filtro. È possibile creare un numero indefinito di filtri.

6.1.6.2.1 Crea una nuova autorità di certificazione

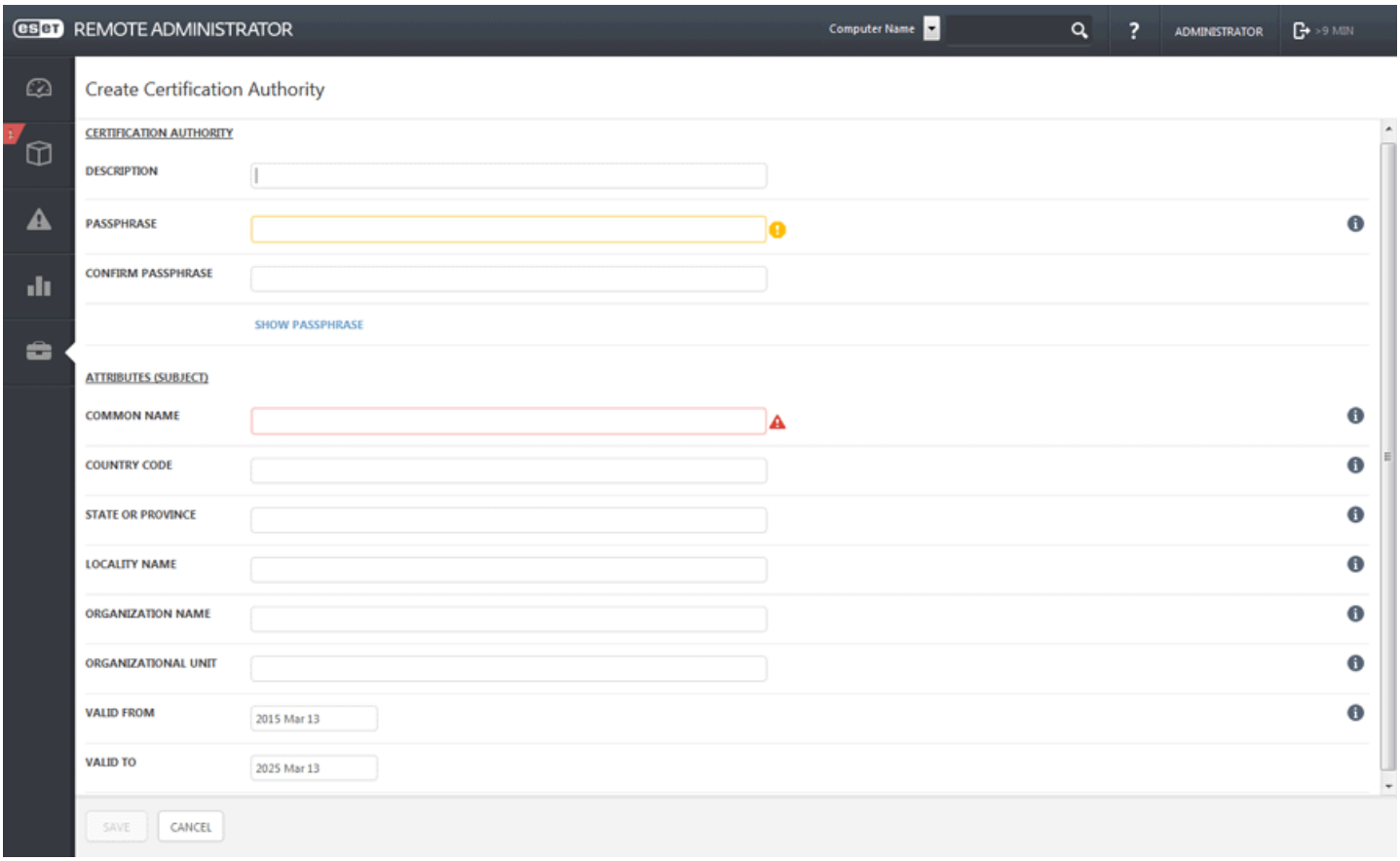
Per creare una nuova autorità, accedere ad **Amministrazione** > **Certificati** > **Autorità di certificazione** e fare clic su **Azione** > **+ Nuova...** o **Nuova** nella parte inferiore della pagina.

Autorità di certificazione

Immettere una **Descrizione** dell'autorità di certificazione e selezionare una **Passphrase**. La **Passphrase** deve contenere almeno 12 caratteri.

Attributi (oggetto)

1. Immettere un **Nome comune** (nome) dell'autorità di certificazione. Scegliere un nome univoco per differenziare più autorità di certificazione.
   Facoltativamente, è possibile inserire una descrizione sull'autorità di certificazione.
2. Immettere i valori **Valido da** e **Valido fino a** per assicurare che il certificato sia valido.
3. Fare clic su **Salva** per salvare la nuova autorità di certificazione. Sarà ora inserito nell'elenco Autorità di certificazione in **Amministrazione** > **Certificati** > **Autorità di certificazione**, e disponibile per l'uso.



Per gestire l'Autorità di certificazione, selezionare la casella di controllo accanto all'Autorità di certificazione nell'elenco e utilizzare il menu contestuale (fare clic con il pulsante sinistro del mouse su Autorità di certificazione) o il pulsante **Azione** nella parte inferiore della pagina. Sono disponibili le opzioni **Modifica** per modificare l'autorità di certificazione (vedere i passaggi illustrati in precedenza), **Elimina** per eliminarla completamente o **Esporta chiave pubblica**.

Esporta una chiave pubblica da un'autorità di certificazione

1. Selezionare l'autorità di certificazione che si desidera utilizzare dall'elenco e selezionare la casella di controllo accanto ad essa.
2. Selezionare **Esporta chiave pubblica** nel menu contestuale. La chiave pubblica sarà esportata come file *der*. Selezionare un nome per la chiave pubblica e fare clic su **Salva**.

NOTA: se si elimina l'autorità di certificazione ERA predefinita e se ne crea una nuova, non funzionerà. Sarà infatti necessario assegnarla anche alla macchina del server ERA e riavviare il servizio del server ERA.

6.1.7 Diritti di accesso

I diritti di accesso in ERA si suddividono in due principali categorie:

1. Accesso funzionalità
2. Accesso gruppo statico

L'accesso agli elementi appartenenti a ciascuna delle due categorie deve essere garantito a ogni Utente di ERA Web Console.

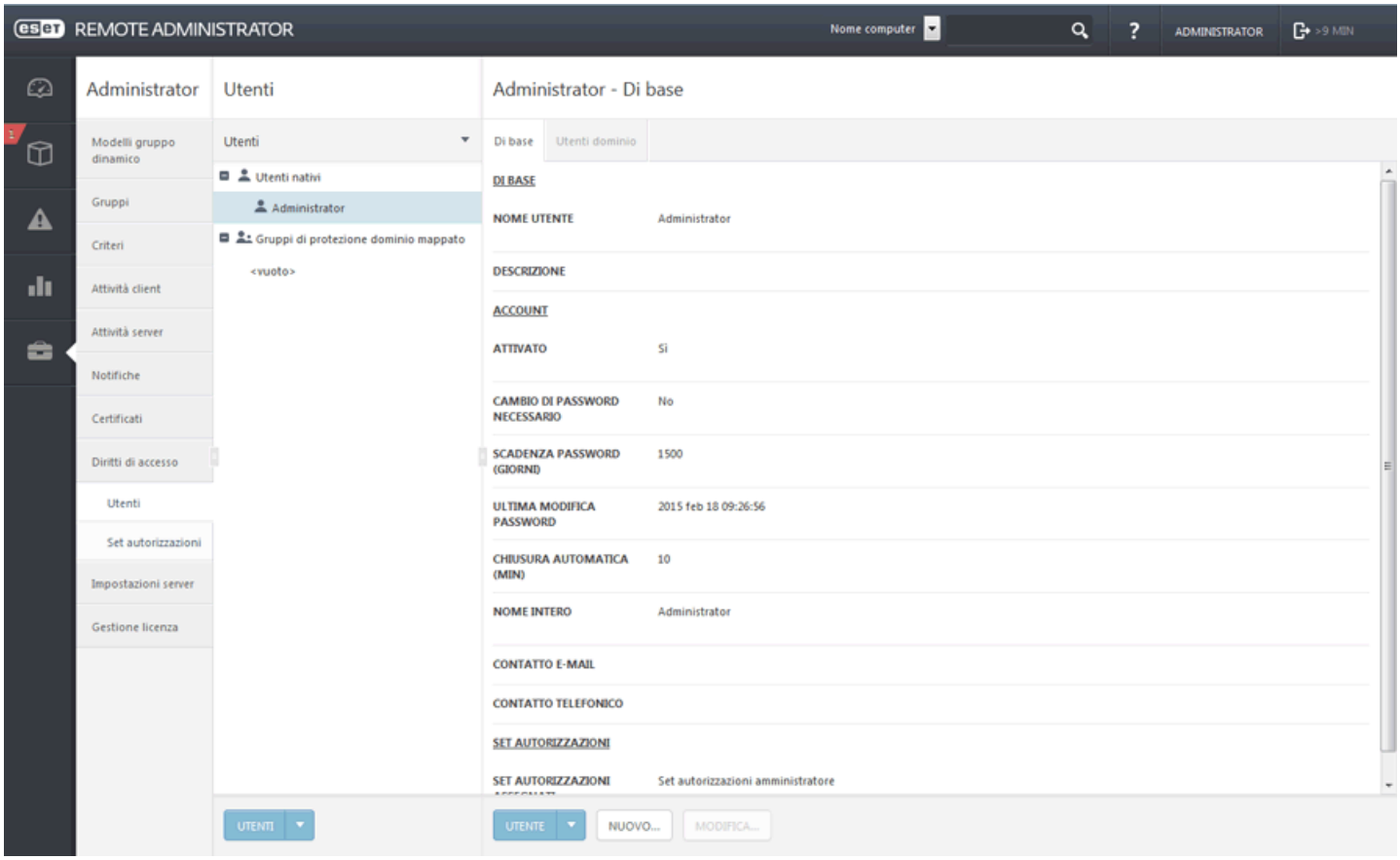
Nella parte superiore è presente l'utente **Amministratore** che ha accesso a tutti gli elementi. La presenza di un numero eccessivo di competenze potrebbe rendere l'utilizzo di questo account piuttosto pericoloso. Si **consiglia vivamente** di creare altri account con diritti di accesso più ristretti tenendo conto esclusivamente delle competenze desiderate.

La gestione degli utenti viene eseguita nell'area Utenti della sezione Amministrazione. Le competenze che è possibile utilizzare sono rappresentate dai Set di autorizzazioni.

6.1.7.1 Utenti

ERA Web Console contiene utenti in possesso di set di autorizzazioni diversi. L'utente con la maggior parte delle autorizzazioni è l'**Amministratore**, che possiede diritti e autorizzazioni completi. Per un utilizzo agevole in Active Directory, gli utenti appartenenti ai gruppi di protezione del dominio hanno diritto di accesso a ERA. Tali utenti sono posizionati accanto agli **Utenti nativi di ERA**, tuttavia, i set di autorizzazioni sono impostati per il gruppo di protezione Active Directory (anziché per utenti individuali, come accade per l'utente nativo).

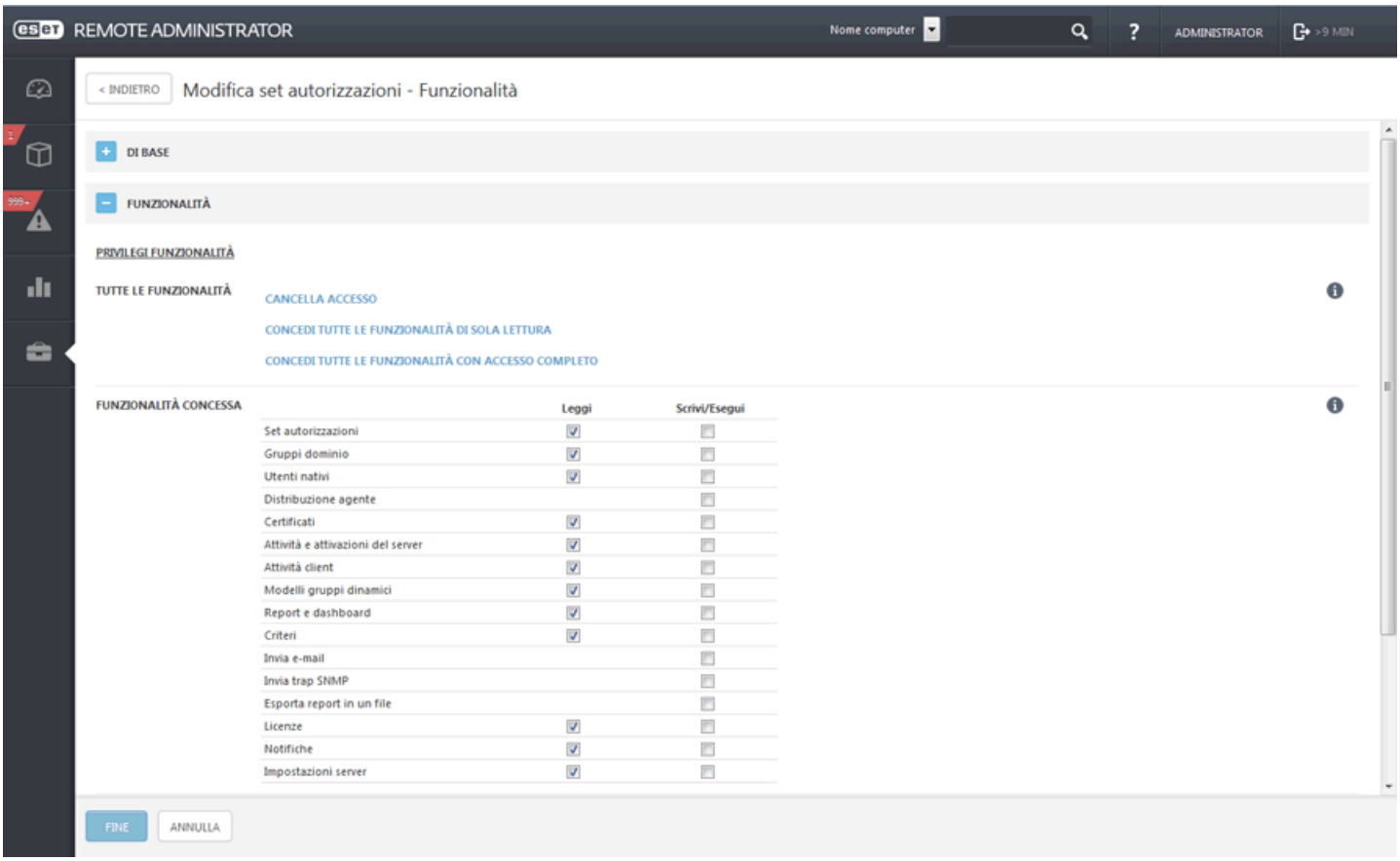
La gestione degli utenti è disponibile nella sezione **Amministrazione** di ERA Web Console.



NOTA: la nuova installazione ERA prevede come unico account l'amministratore (utente nativo).

6.1.7.1.1 Procedura guidata gruppo di protezione dominio mappato

Per accedere alla **Procedura guidata gruppo di protezione di dominio mappato**, accedere ad **Amministrazione** > **Diritti di accesso** > **Gruppi di protezione dominio mappato** > **Nuovo** o semplicemente a **Nuovo** (in caso di selezione del gruppo di protezione del dominio mappato nella struttura ad albero).



Di base

Gruppo dominio

Inserire un **Nome** per il gruppo e, facoltativamente, una descrizione. Il gruppo verrà definito da un **SID gruppo** (identificatore di protezione). Fare clic su **Seleziona** per selezionare un gruppo dall'elenco, quindi su **OK** per confermare.

Account

- Lasciare selezionato **Attivato** per rendere attivo l'utente.
- L'opzione **Chiusura automatica (min)** definisce il periodo di tempo di inattività (in minuti), al termine del quale l'utente verrà disconnesso da ERA Web Console.
- **Indirizzo e-mail** e **Contatto telefonico** sono campi facoltativi concepiti ai fini dell'identificazione dell'utente.

Set autorizzazioni

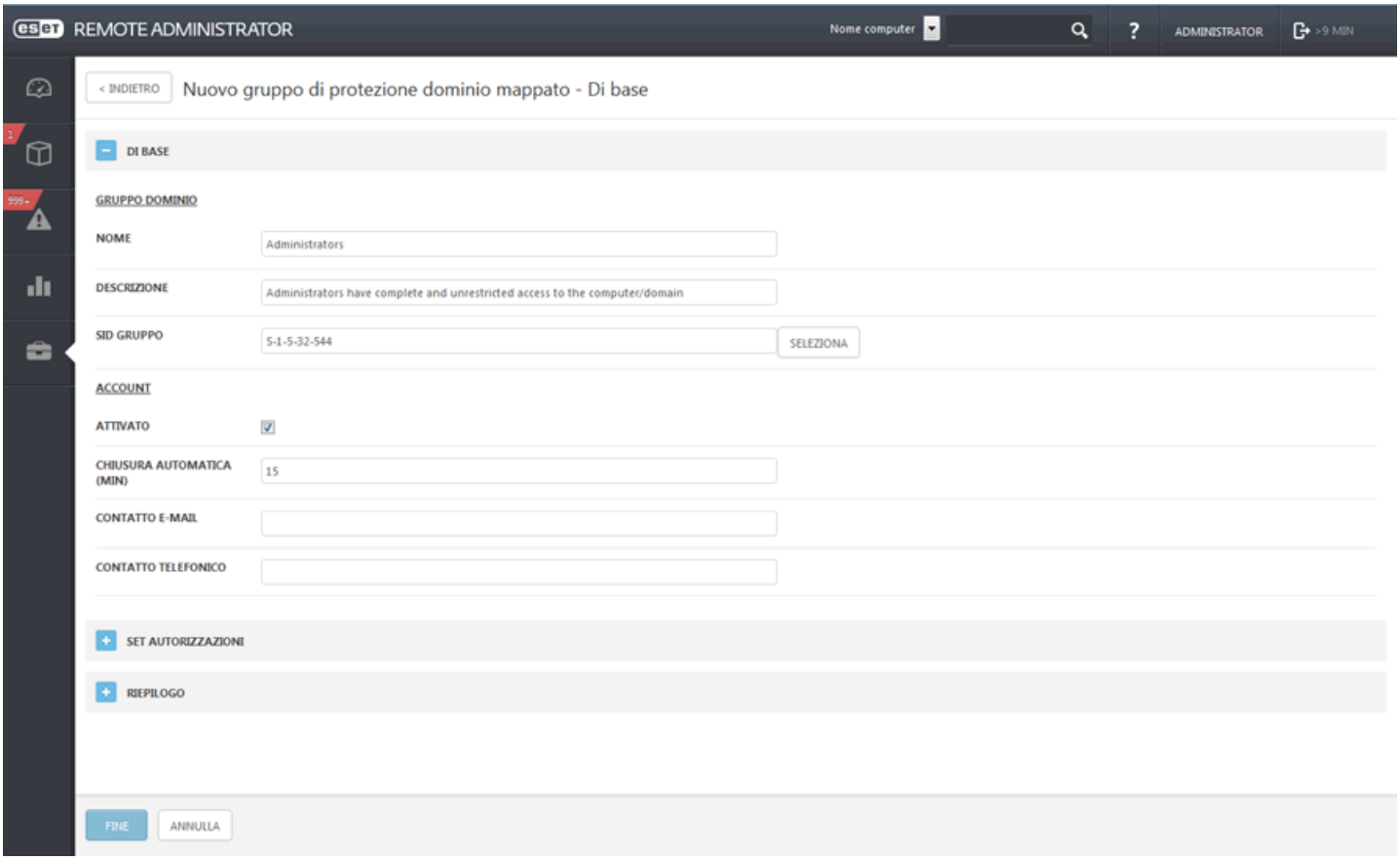
Assegnare le competenze (diritti) all'utente. È possibile utilizzare una competenza predefinita: **Set autorizzazioni revisore** (simile ai diritti di sola lettura) o **Set autorizzazioni amministratore** (simile all'accesso completo) oppure è possibile utilizzare un set di autorizzazioni personalizzato.

Riepilogo

Rivedere le impostazioni configurate per questo utente e fare clic su **Fine** per creare il gruppo.

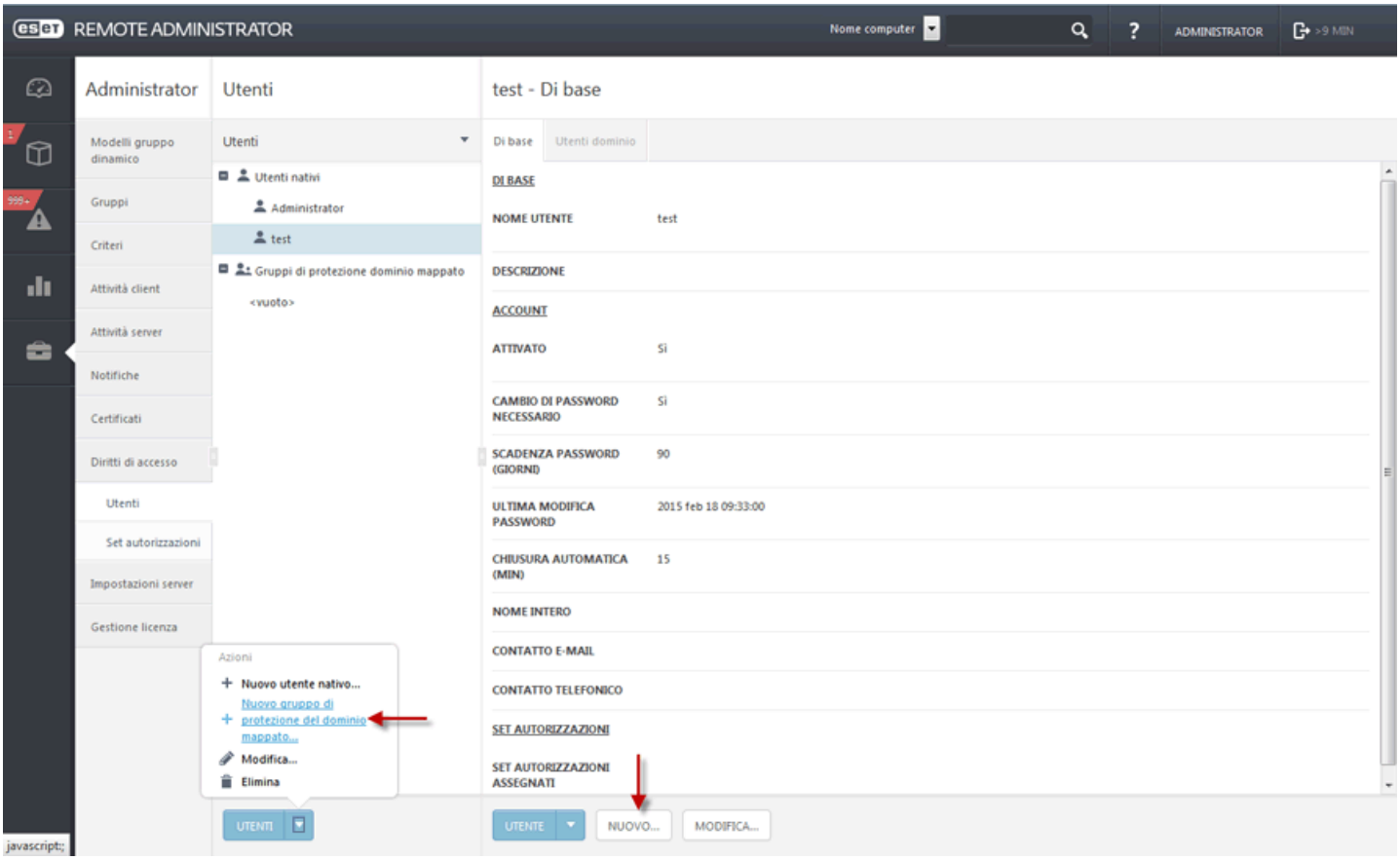
6.1.7.1.2 Procedura guidata utente nativo

Per accedere alla **Procedura guidata utente nativo**, accedere ad **Amministrazione** > **Diritti di accesso** > **Utente** > **Utenti** o **Nuovo** nella parte inferiore della pagina.



6.1.7.1.3 Crea un utente nativo

Per creare un nuovo Utente nativo, nella scheda **Amministrazione** fare clic su **Diritti di accesso** > **Utente** , quindi su **Utenti** o **Nuovo** nella parte inferiore della pagina.



Di base

Inserire un **Nome utente** e una **Descrizione** facoltativa del nuovo utente.

Autenticazione

La password per l'utente deve contenere almeno 8 caratteri. La password non deve contenere il nome utente.

Account

- Lasciare selezionato **Attivato**, fatta eccezione per il caso in cui l'utente desideri che l'account resti inattivo (destinato a utilizzi successivi).
- Lasciare deselezionato **Cambio di password necessario** (la selezione di questa opzione forzerà la modifica della password da parte dell'utente al primo accesso a ERA Web Console).
- L'opzione **Scadenza password** definisce il numero di giorni di validità della password, al termine dei quali è necessario modificarla.
- L'opzione **Chiusura automatica (min)** definisce il periodo di tempo di inattività (in minuti), al termine del quale l'utente verrà disconnesso dalla console Web.
- Per facilitare l'identificazione dell'utente, definire il **Nome completo**, l'**E-mail contatto** e il **Contatto telefonico**.

Set autorizzazioni

Assegnare le competenze (diritti) all'utente. È possibile selezionare una competenza predefinita: **Set autorizzazioni revisore** (simile ai diritti di sola lettura) o **Set autorizzazioni amministratore** (simile all'accesso completo) oppure è possibile utilizzare un set di autorizzazioni personalizzato.

Riepilogo

Rivedere le impostazioni configurate per questo utente e fare clic su **Fine** per creare l'account.

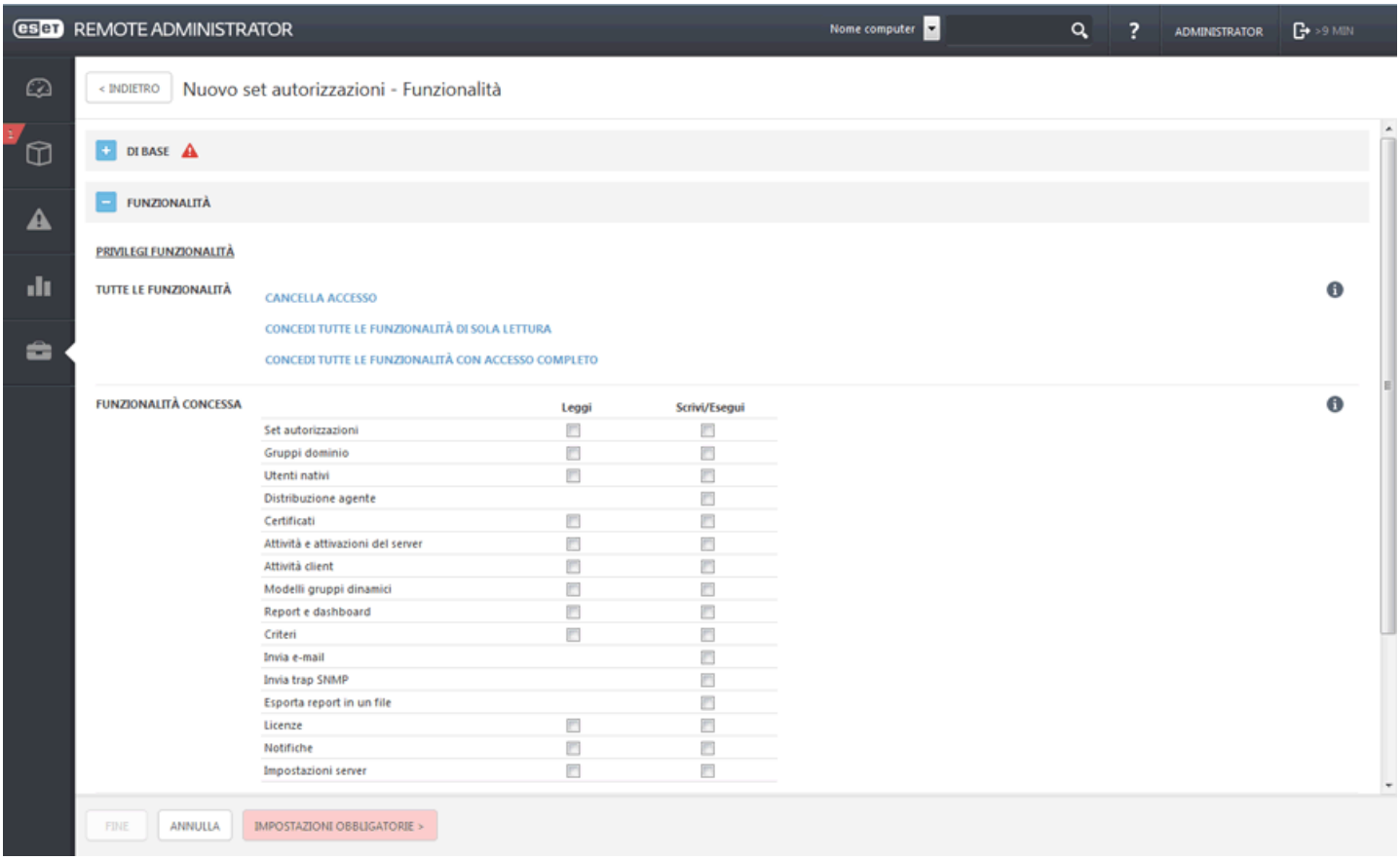
6.1.7.1.3.1 Crea nuovo account amministratore

Per creare un secondo account Amministratore, seguire i passaggi per creare un account utente nativo e assegnare il set autorizzazioni amministratore a tale account.

6.1.7.1.4 Mappa gruppo su gruppo di protezione dominio

È possibile eseguire il mapping di un gruppo di protezione del dominio sul server ERA e consentire agli utenti esistenti (membri dei gruppi di protezione del dominio) di diventare utenti di ERA Web Console.

Fare clic su **Amministrazione** > **Diritti di accesso** > **Gruppi di protezione dominio mappato** > **Nuovo** o semplicemente su **Nuovo** (in caso di selezione del gruppo di protezione del dominio mappato nella struttura ad albero).



Di base

Gruppo dominio

Inserire un **Nome** per il gruppo e, facoltativamente, una descrizione. Il gruppo verrà definito da un **SID gruppo** (identificatore di protezione). Fare clic su **Seleziona** per selezionare un gruppo dall'elenco, quindi su **OK** per confermare.

Account

- Lasciare selezionato **Attivato** per rendere attivo l'utente.
- L'opzione **Chiusura automatica (min)** definisce il periodo di tempo di inattività (in minuti), al termine del quale l'utente verrà disconnesso dalla console Web.
- **Indirizzo e-mail** e **Contatto telefonico** sono campi facoltativi concepiti ai fini dell'identificazione dell'utente.

Set autorizzazioni

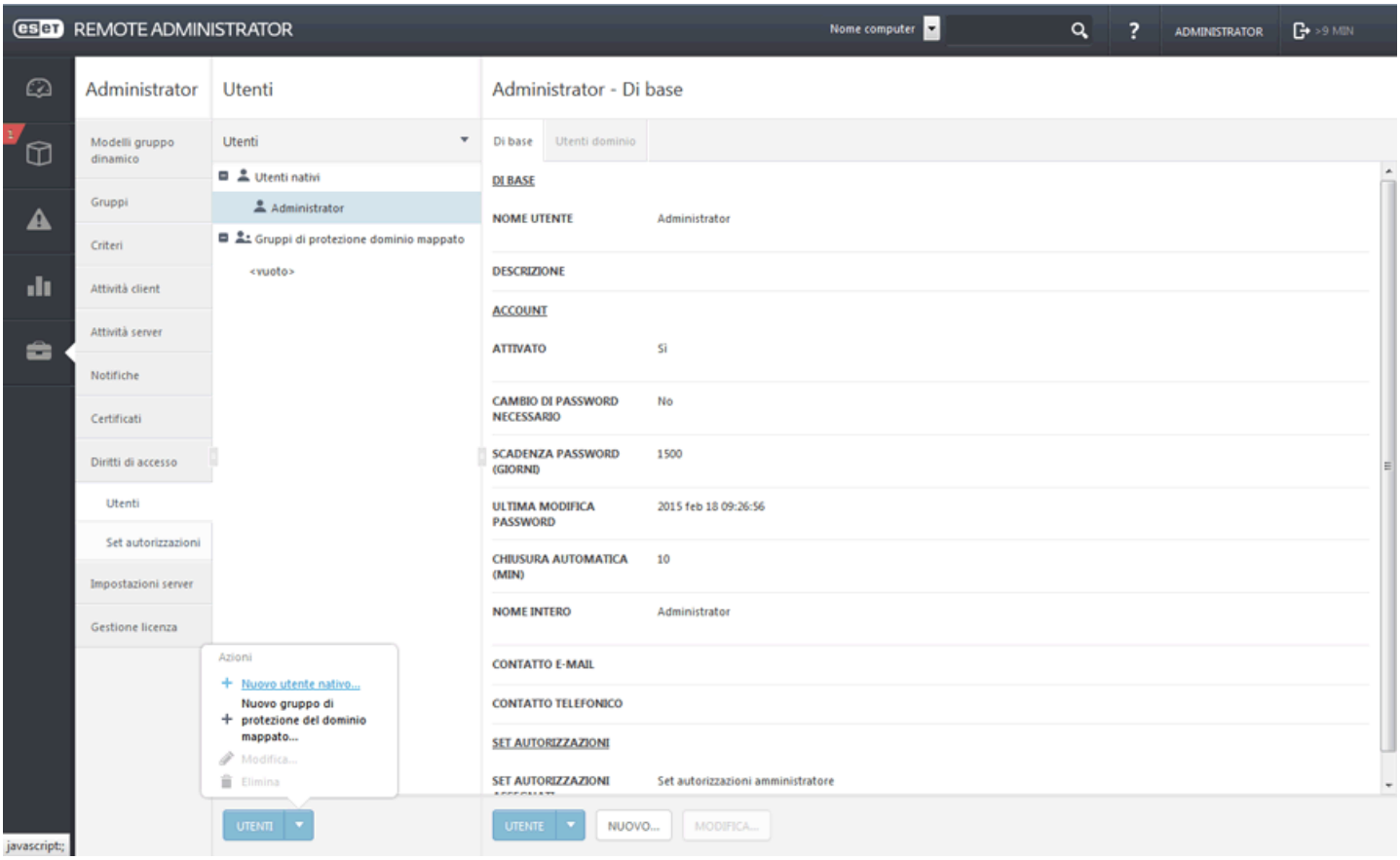
Assegnare le competenze (diritti) all'utente. È possibile utilizzare una competenza predefinita: **Set autorizzazioni revisore** (simile ai diritti di sola lettura) o **Set autorizzazioni amministratore** (simile all'accesso completo) oppure è possibile utilizzare un set di autorizzazioni personalizzato.

Riepilogo

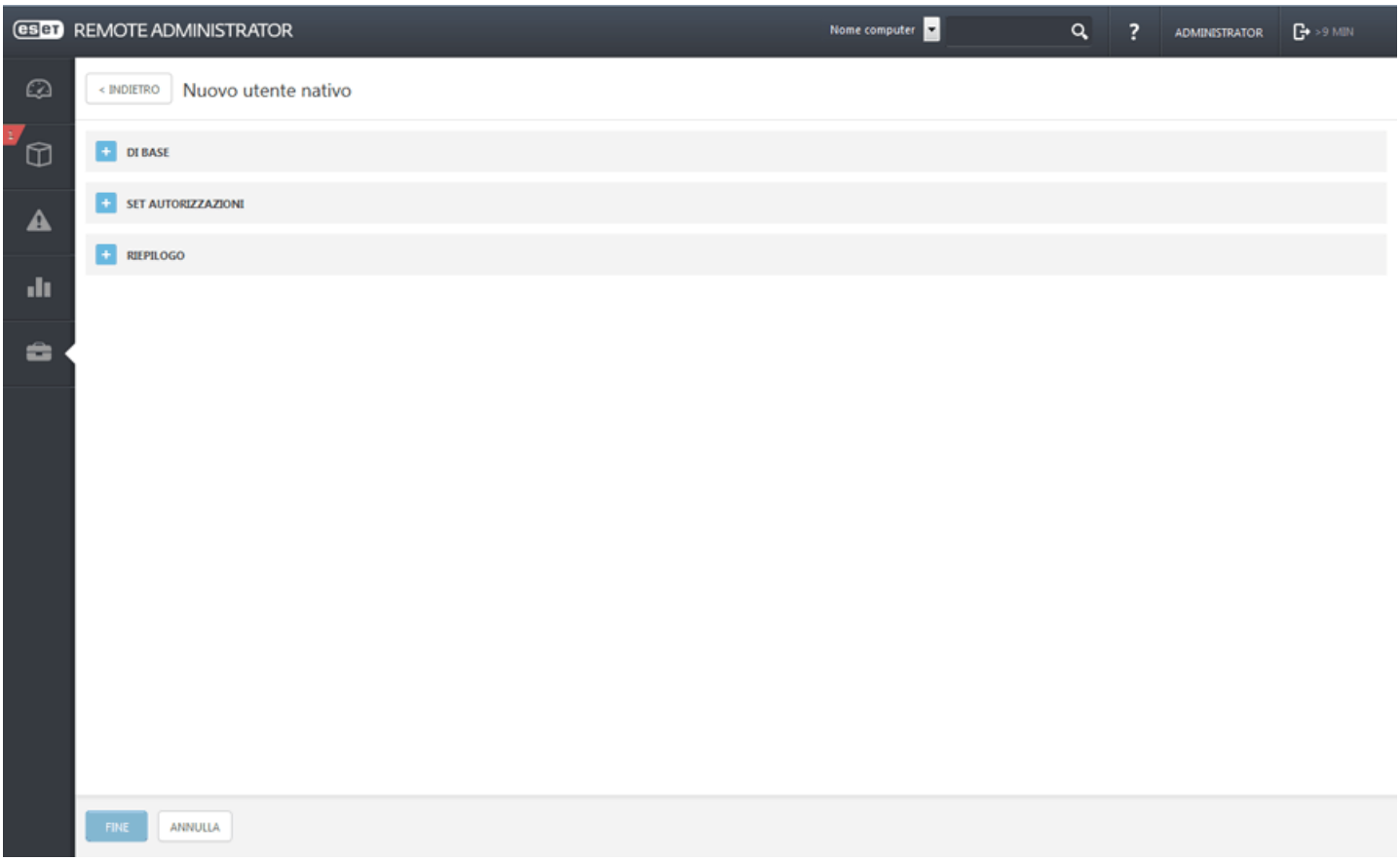
Rivedere le impostazioni configurate per questo utente e fare clic su **Fine** per creare il gruppo.

6.1.7.1.5 Assegna utente a un set di autorizzazioni

Accedere a **Amministrazione** > **Diritti di accesso** > **Set autorizzazioni**, quindi fare clic su **Modifica** per assegnare un utente a uno specifico set di autorizzazioni. Per ulteriori informazioni, consultare Gestisci set di autorizzazioni.



Nella sezione **Utenti**, modificare un utente specifico facendo clic su **Modifica...** e spuntare la casella di controllo accanto a uno specifico set di autorizzazioni nella sezione **Set autorizzazioni non assegnati (disponibili)**.



6.1.7.2 Set autorizzazioni

Un set di autorizzazioni rappresenta un insieme di autorizzazioni per gli utenti che accedono a ERA Web Console e definisce ciò che gli utenti possono fare o visualizzare nella console Web. Gli Utenti nativi possiedono le proprie autorizzazioni, mentre gli utenti del dominio possiedono le autorizzazioni del relativo gruppo di protezione mappato.

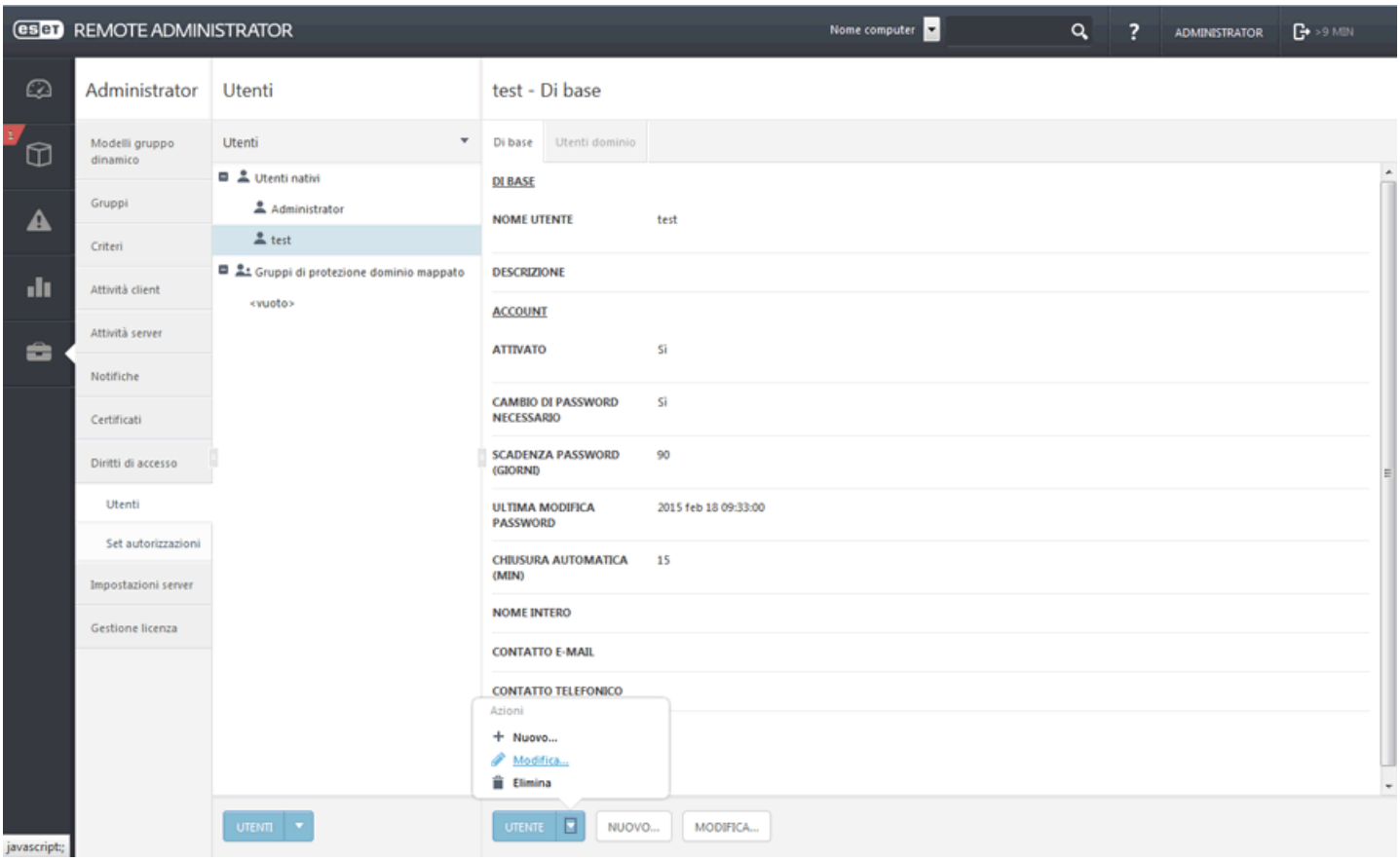
La autorizzazioni di ERA Web Console sono suddivise in varie categorie, ad esempio Utenti nativi, Certificati, Criteri e così via. Per ciascuna funzionalità, un determinato set di autorizzazioni può consentire l'accesso Di sola lettura o Scrittura/esecuzione.

Le autorizzazioni **Di sola lettura** sono adatte agli utenti addetti al controllo che possono visualizzare i dati ma non modificarli.

Le autorizzazioni di **Scrittura/esecuzione** consentono agli utenti con questo privilegio di modificare o eseguire, se possibile, i relativi oggetti (ad esempio, esecuzione di attività).

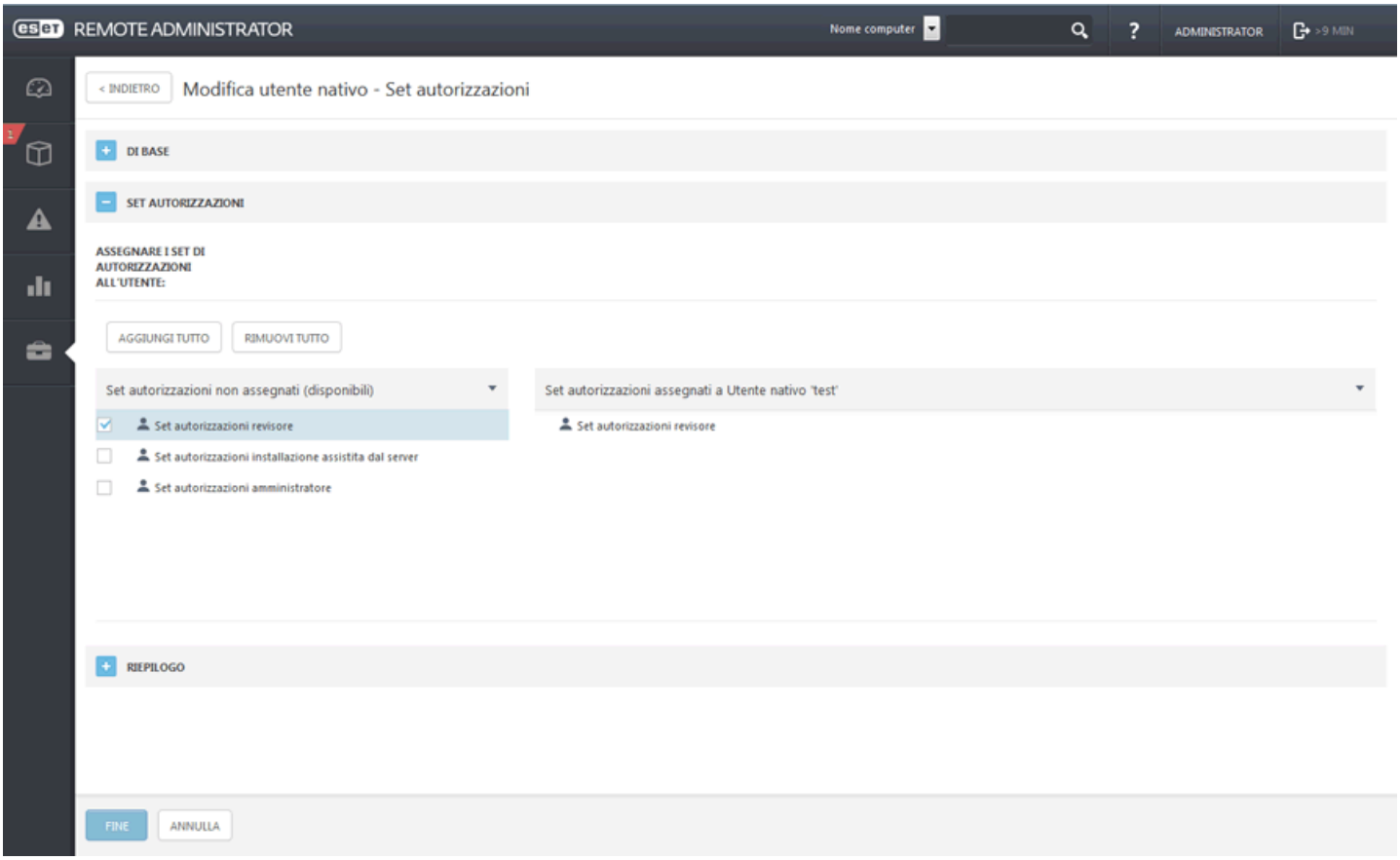
Oltre alle autorizzazioni relative alla funzionalità ERA, gli utenti possono accedere a Gruppi statici. Nello specifico, ogni utente può accedere a **tutti** o a **sottoinsiemi di Gruppi statici**. L'accesso a uno specifico Gruppo statico comporta automaticamente l'accesso ai relativi sottogruppi. In tal caso:

- l'accesso **Di sola lettura** comporta l'accesso a tutti i computer dell'elenco.
- L'autorizzazione relativa a **Scrittura/esecuzione** consente all'utente di modificare i computer all'interno del Gruppo statico, nonché di assegnare Attività client e Criteri.



6.1.7.2.1 Procedura guidata set di autorizzazioni

Per aggiungere un nuovo set di autorizzazioni, fare clic su **Set autorizzazioni** > **Nuovo** o semplicemente su **Nuovo**.

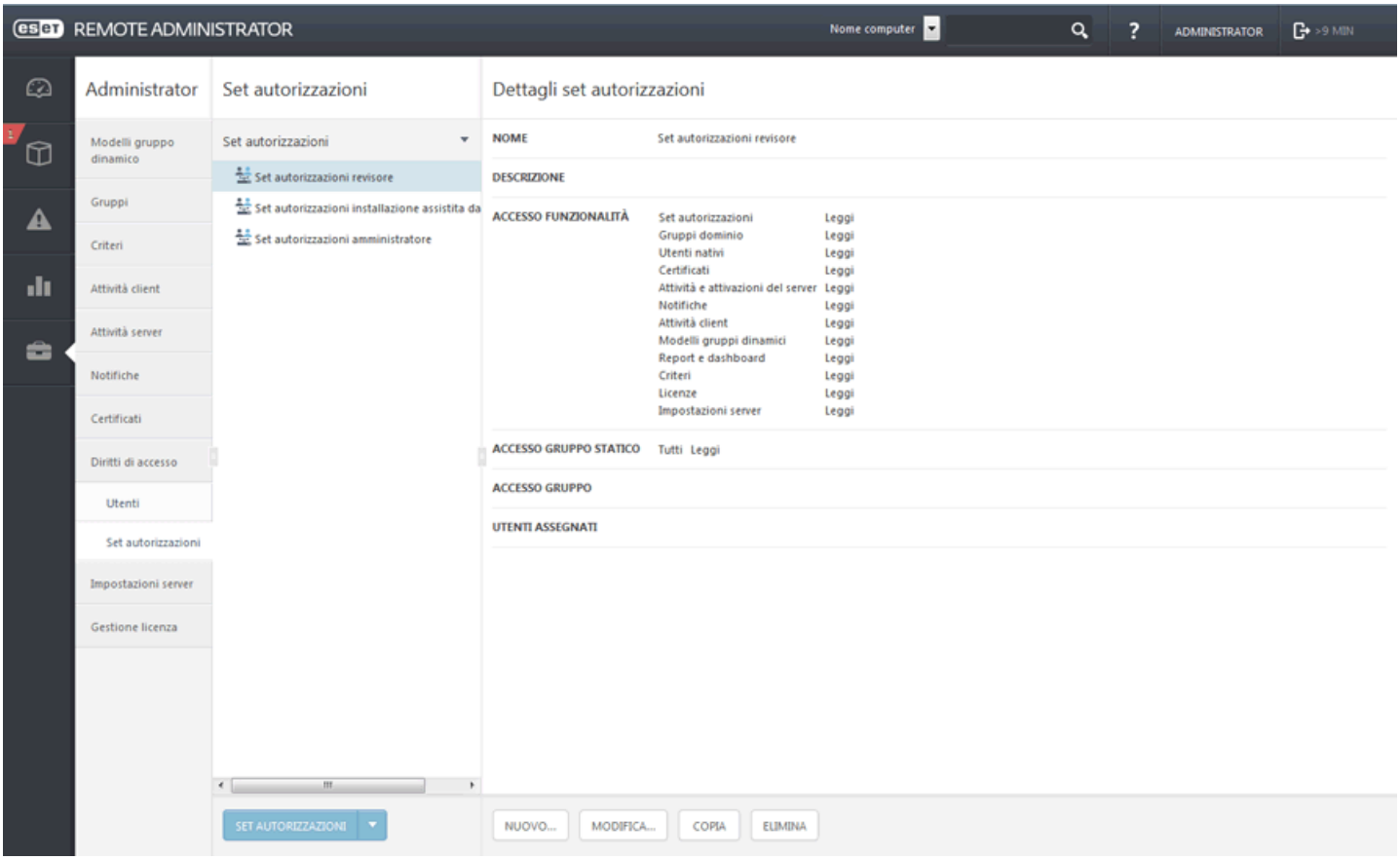


6.1.7.2.2 Gestisci set di autorizzazioni

Per modificare uno specifico set di autorizzazioni, fare clic su di esso, quindi su **Modifica**. Fare clic su **Copia** per creare un set di autorizzazioni duplicato che è possibile modificare e assegnare a un utente specifico.

Di base

Inserire un **Nome** per il set (impostazione obbligatoria) e, facoltativamente, una **Descrizione**.



Funzionalità

Selezionare i singoli moduli ai quali si desidera garantire l'accesso. L'utente in possesso di questa competenza avrà accesso a queste specifiche attività. È inoltre possibile **Concedere la sola lettura a tutti i moduli** e **Concedere l'accesso completo a tutti i moduli**. Tuttavia, le seguenti competenze sono già esistenti: **Competenza amministratore** (accesso completo) e **Competenza revisore** (sola lettura). La concessione di diritti di **Lettura/esecuzione** determina la concessione automatica di diritti di **Lettura**.

Gruppi statici

È possibile aggiungere un Gruppo statico (o Gruppi statici multipli) che assumeranno questa competenza (e i diritti definiti nella sezione **Moduli**) e concedere a tutti i Gruppi statici un accesso di sola lettura o completo. È possibile aggiungere esclusivamente Gruppi statici, in quanto i set di autorizzazioni concessi sono fissi per specifici utenti o gruppi.

Utenti

Tutti gli utenti disponibili sono elencati sulla sinistra. Selezionare utenti specifici o tutti gli utenti utilizzando il pulsante **Aggiungi tutto**. Gli utenti assegnati sono elencati sulla destra.

Riepilogo

Rivedere le impostazioni configurate per questa competenza e fare clic su **Fine**.

6.1.8 Impostazioni server

In questa sezione, è possibile configurare specifiche impostazioni del server ESET Remote Administrator stesso.

Connessione

- **Porta Remote Administrator (richiede riavvio)**: porta per la connessione tra il server e uno o più agenti ESET Remote Administrator. Per essere effettiva, la modifica di questa opzione richiede il riavvio del servizio del server ERA.
- **Porta ERA Web Console (richiede riavvio)** : porta per la connessione tra la console Web e il server ERA.
- **Certificato**: qui è possibile gestire i certificati. Per ulteriori informazioni, consultare il capitolo Certificati del peer.

Aggiornamenti

- **Intervallo di aggiornamento**: intervallo in cui verranno ricevuti gli aggiornamenti. È impossibile selezionare un intervallo periodico e configurare le impostazioni oppure utilizzare un'espressione CRON.
- **Server di aggiornamento**: server di aggiornamento da cui il server ERA riceve gli aggiornamenti dei prodotti di protezione e i componenti ERA.
- **Tipo di aggiornamento**: selezionare il tipo di aggiornamento che si desidera ricevere. tra aggiornamenti periodici, pre-rilascio o ritardati. Si sconsiglia di selezionare l'opzione degli aggiornamenti pre-rilascio per i sistemi di produzione, in quanto tale operazione potrebbe costituire un rischio.

Impostazioni avanzate

- **Proxy HTTP**: è possibile utilizzare un server proxy per consentire la connessione a Internet.
- **Server SMTP**: è possibile utilizzare un server SMTP per ricevere o inviare vari messaggi. In questa sezione, è possibile configurare le impostazioni del server SMTP.
- **Archivio**: posizione dell'archivio in cui sono memorizzati tutti i file di installazione.
- **Registrazione**: è possibile impostare il livello di dettaglio del rapporto che determina la quantità di informazioni che verranno raccolte e registrate - da **Monitoraggio** (livello informativo) a **Irreversibile** (informazioni critiche più importanti).
- **Pulizia del database**: per prevenire un sovraccarico del database, è possibile utilizzare questa opzione per pulire periodicamente i rapporti.

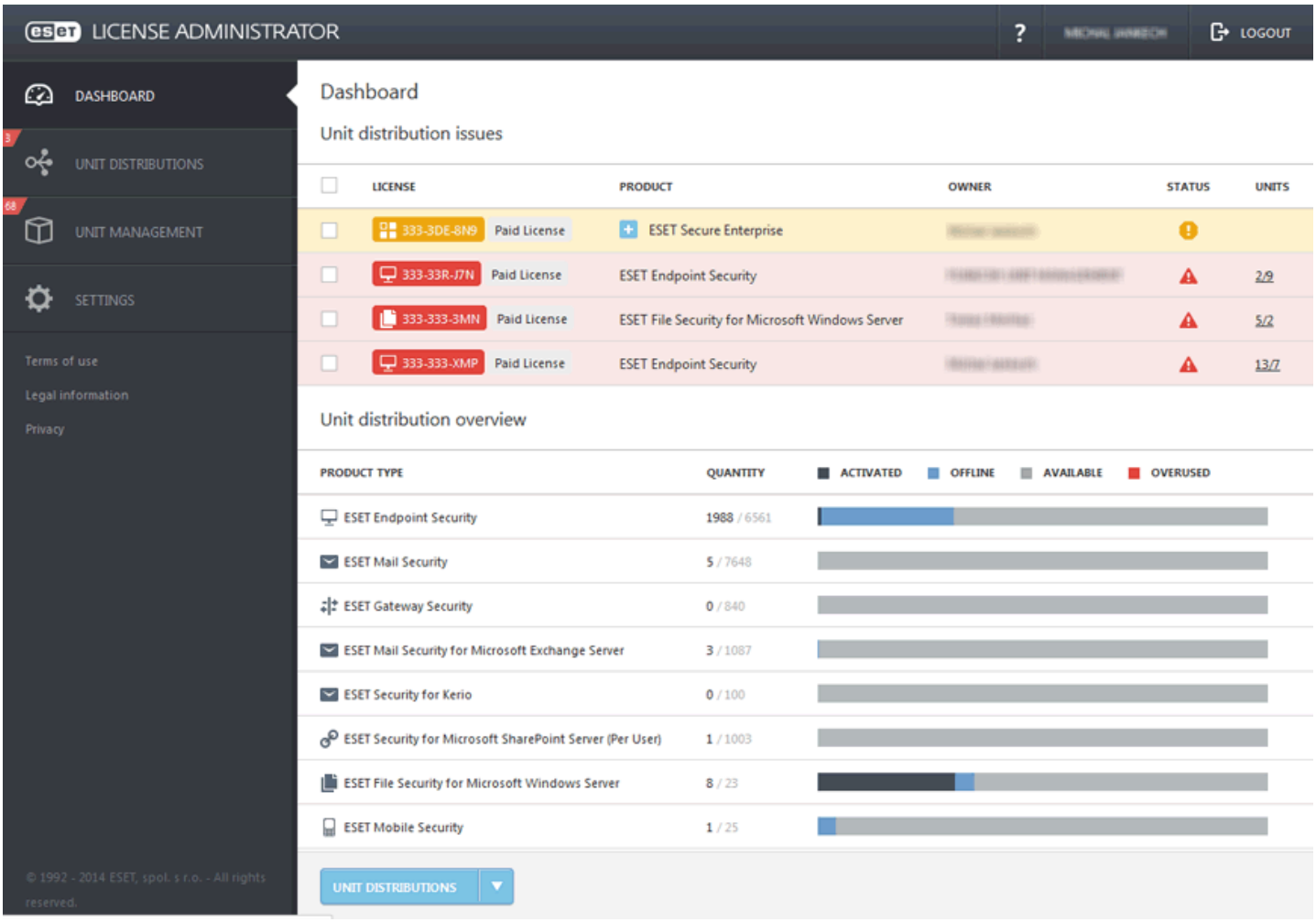
6.1.9 Gestione licenza

A partire dalla versione 6 di ESET Remote Administrator, è disponibile un sistema di gestione delle licenze ESET completamente nuovo.

Il nome utente e la password vengono sostituiti da una **Chiave di licenza**/un **ID pubblico**: una **Chiave di licenza** è una stringa univoca che viene utilizzata per identificare il proprietario della licenza e per l'attivazione della stessa. L'**ID pubblico** è una breve stringa utilizzata per identificare la licenza su un sistema di terze parti (ad esempio, il **Security Admin** responsabile della Distribuzione delle unità).

Un **Security Admin** è una persona che gestisce le licenze e potrebbe non corrispondere all'effettivo **Proprietario della licenza**. Il proprietario della licenza delega una licenza a un security admin (ovvero, lo autorizza) che, in caso di accettazione, potrà gestirla (apportare modifiche, associare unità e così via). Un security admin può utilizzare la licenza per attivare prodotti ESET (associare un'unità).

Le licenze possono essere gestite da questa sezione oppure on-line facendo clic su **Apri ELA** (ESET License Administrator) o utilizzando l'Interfaccia Web di ESET License Administrator (vedere la sezione Security Admin).



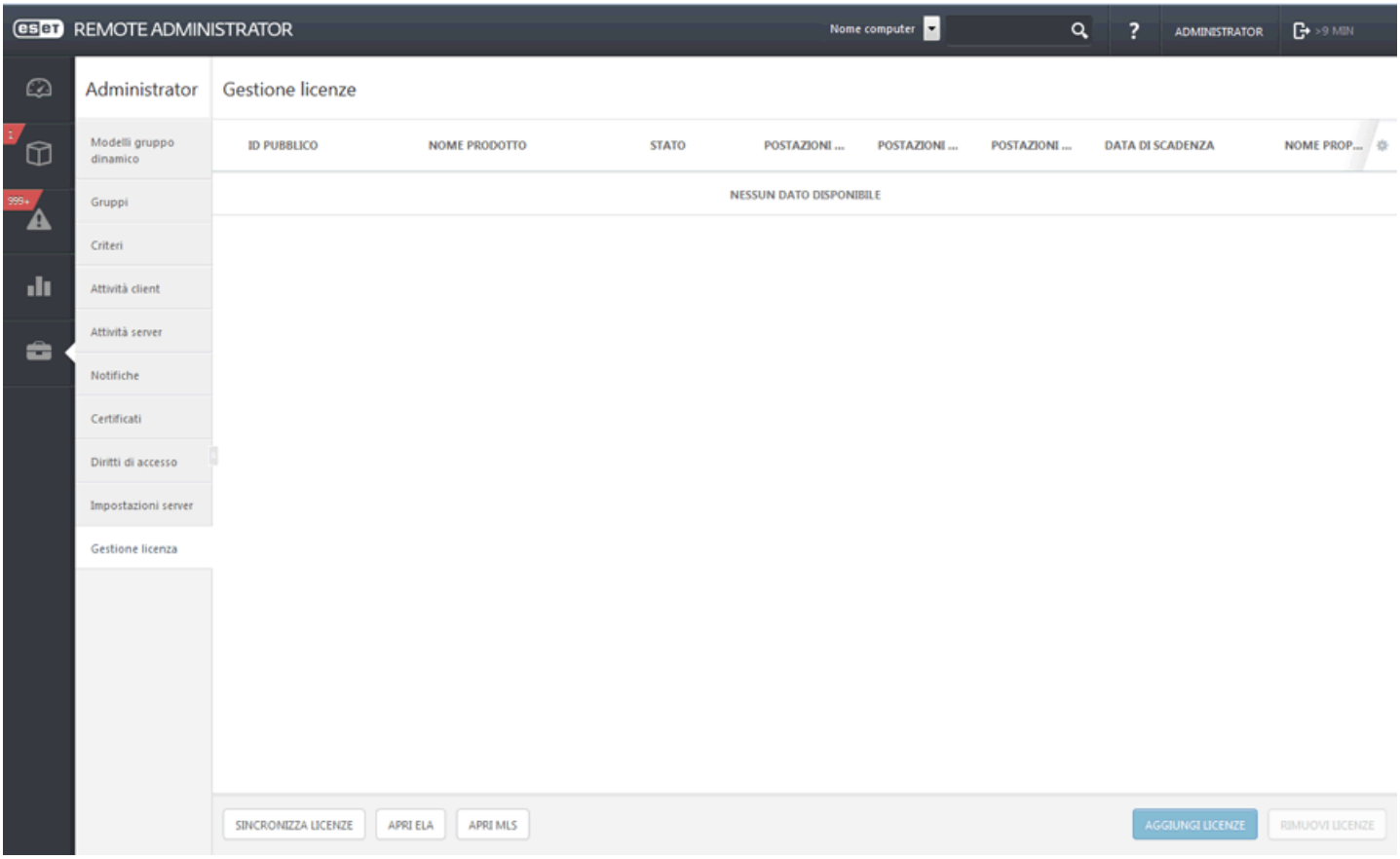
La sezione Gestione licenza in ESET Remote Administrator 6 è accessibile dal menu principale in **Amministrazione** > **Gestione licenza**.

Le licenze possono essere distribuite ai prodotti di protezione ESET da ERA tramite due attività:

- L'attività di installazione del software
- L'attività di attivazione del prodotto

Le licenze sono identificate in modo univoco dal relativo ID pubblico. In ciascuna di esse compaiono le seguenti informazioni:

- il **Nome del prodotto** di protezione per il quale è stata concepita la licenza
- lo **Stato** complessivo della licenza (se la licenza è scaduta, soggetta a un utilizzo eccessivo o a rischio di scadenza o di utilizzo eccessivo, verrà visualizzato un messaggio di avviso qui)
- il numero di **Unità** che è possibile attivare con questa licenza
- la data di scadenza della licenza
- il **Nome del proprietario** e del **Contatto** associati alla licenza.



Sincronizza licenze

La sincronizzazione delle licenze con ESET License Administrator viene eseguita automaticamente una volta a settimana. Se si apportano modifiche in ESET License Administrator e si desidera visualizzare subito le informazioni sulla licenza corrente in ERA anziché attendere la successiva sincronizzazione automatica, fare clic sul pulsante **Sincronizza licenze**.

Aggiungi licenza o chiave di licenza

Fare clic su Aggiungi licenze e selezionare il metodo che si desidera utilizzare per aggiungere la/e nuova/e licenza/e:

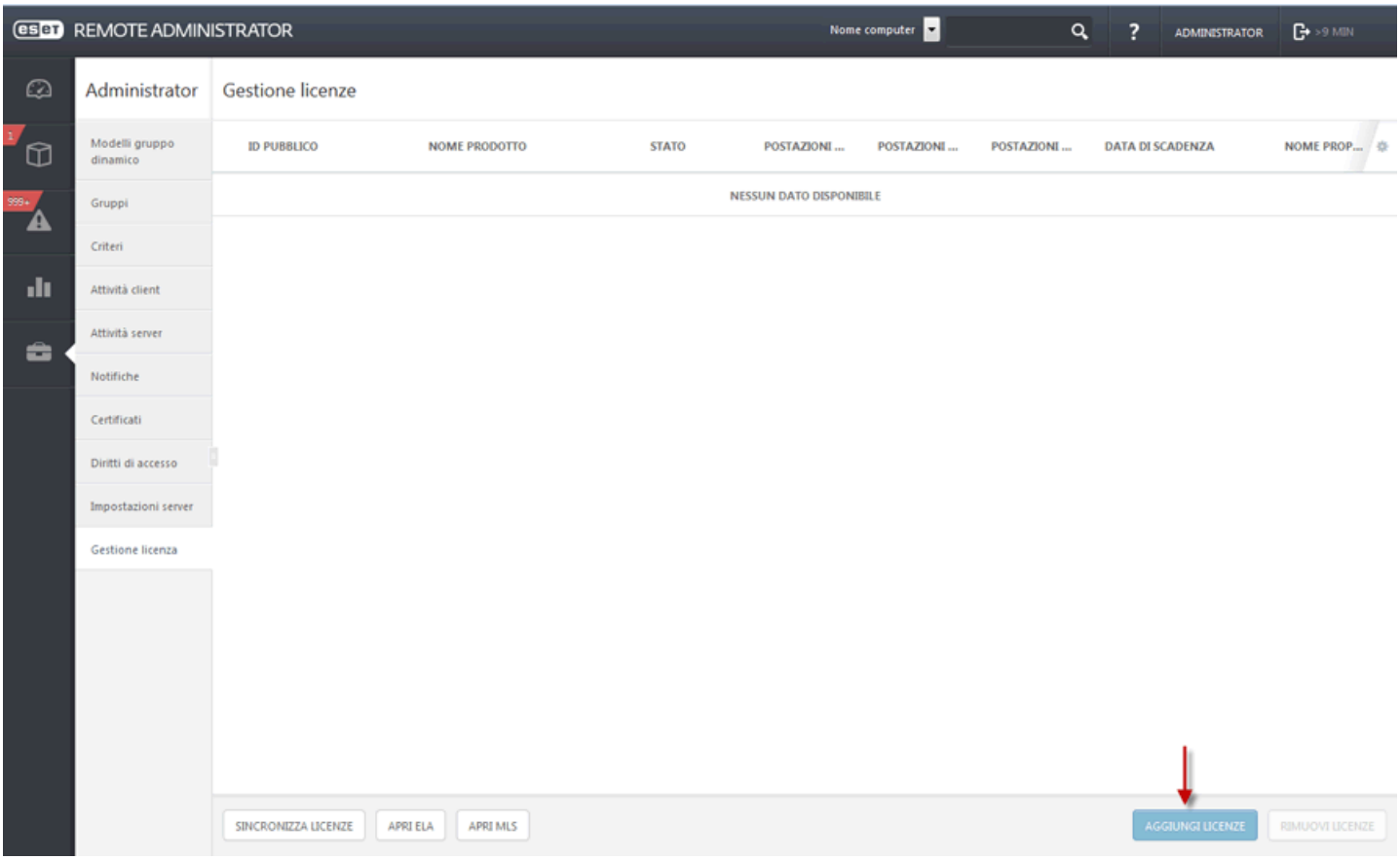
1. Chiave di licenza: inserire la chiave di una licenza valida e fare clic su **Aggiungi licenza**. La chiave di licenza verrà verificata in base al server di attivazione e aggiunta all'elenco.
2. Credenziali Security Admin: collegare un account security admin e tutte le relative licenze alla sezione **Gestione licenze**.
3. File di licenza: aggiungere un file di licenza (.lf) e fare clic su **Aggiungi licenza**. Il file di licenza verrà verificato e la licenza aggiunta all'elenco.

Rimuovi licenze

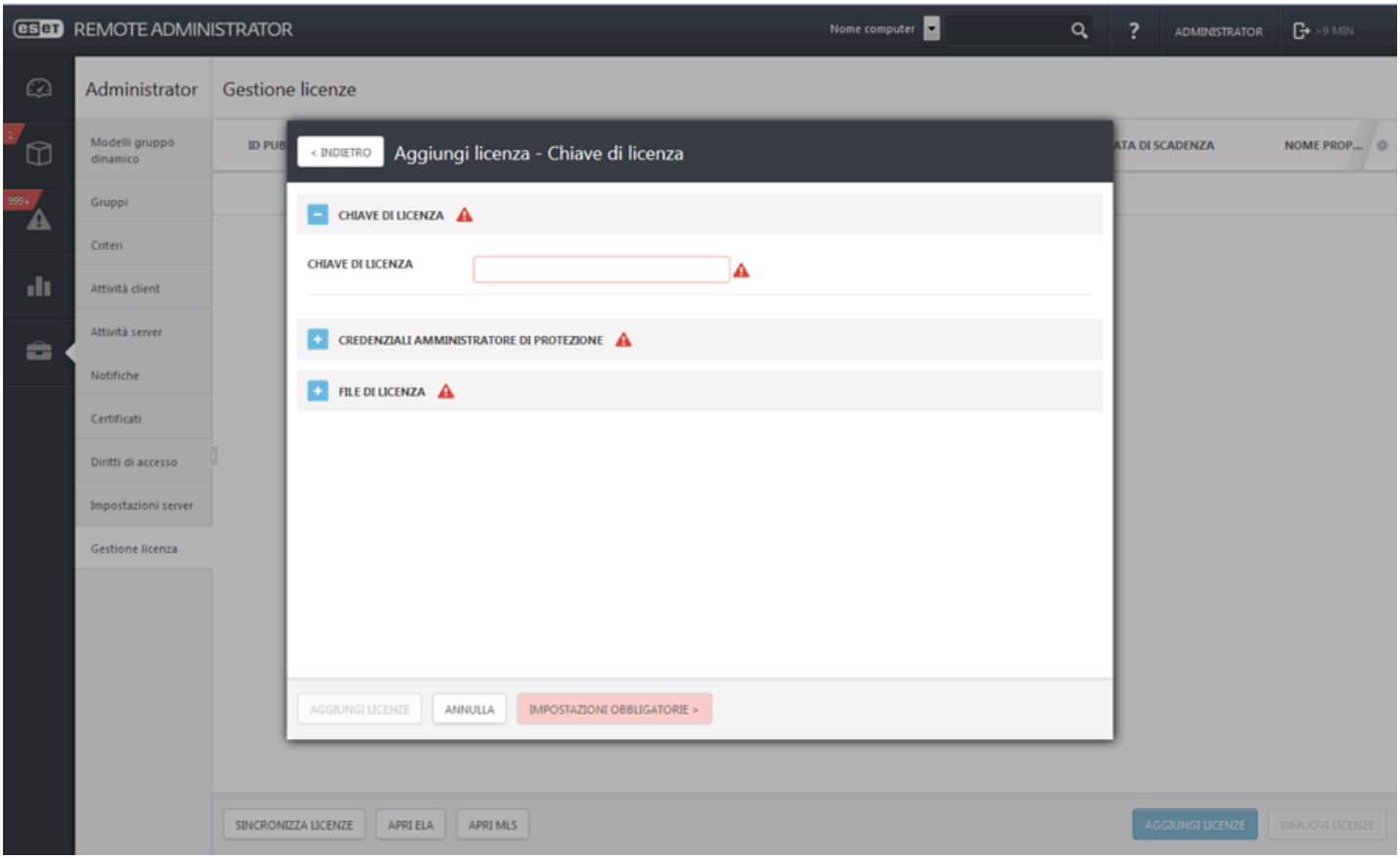
Selezionare una licenza dall'elenco indicato in precedenza e fare clic su questa opzione per rimuoverla completamente. All'utente verrà richiesto di confermare l'azione. La rimozione della licenza non determina la disattivazione del prodotto. Il prodotto ESET rimane attivato anche in caso di eliminazione della licenza in ERA License Management.

6.1.9.1 Attivazione

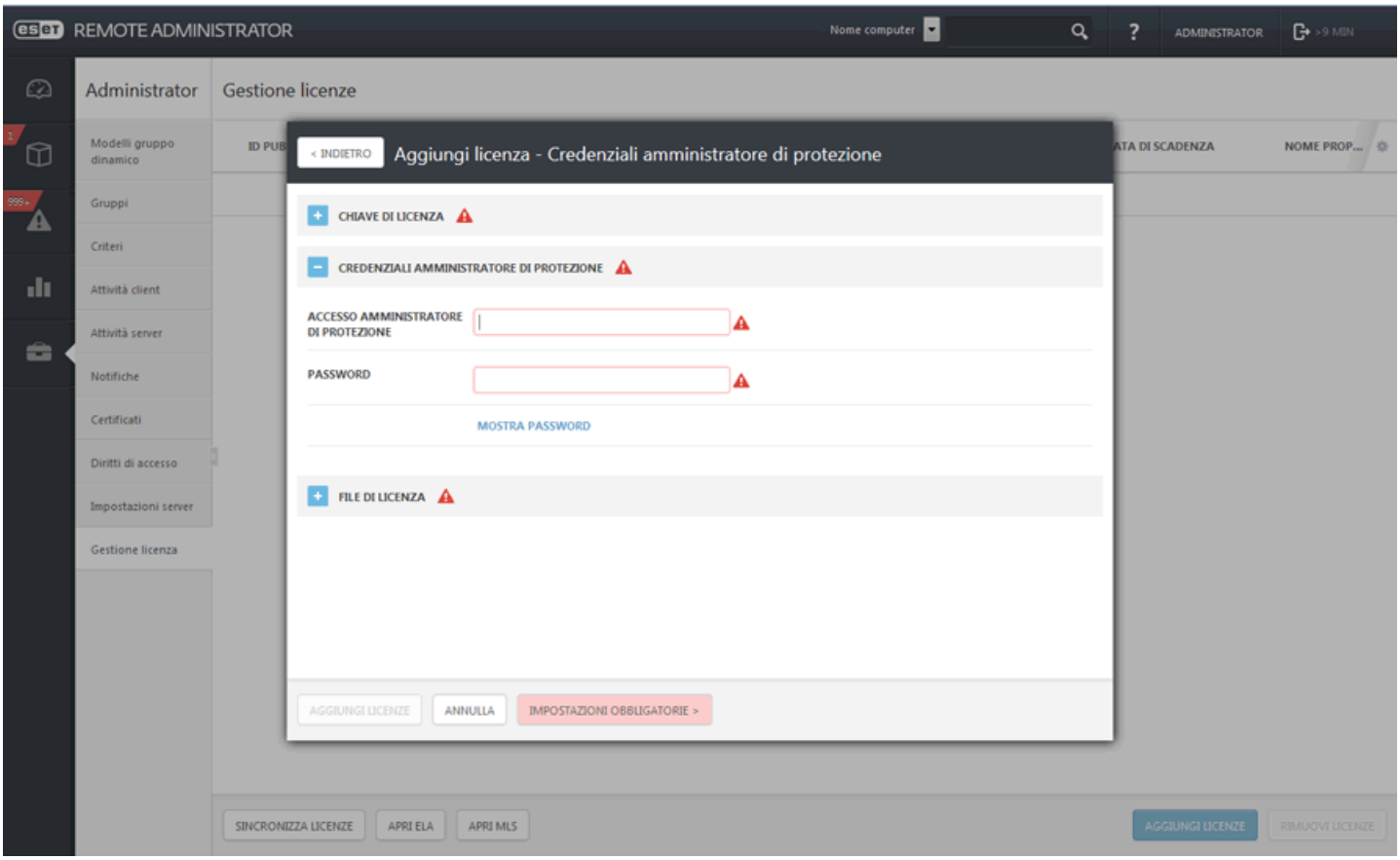
Accedere ad **Amministrazione** > **Gestione licenza** e fare clic su **Aggiungi licenze**.



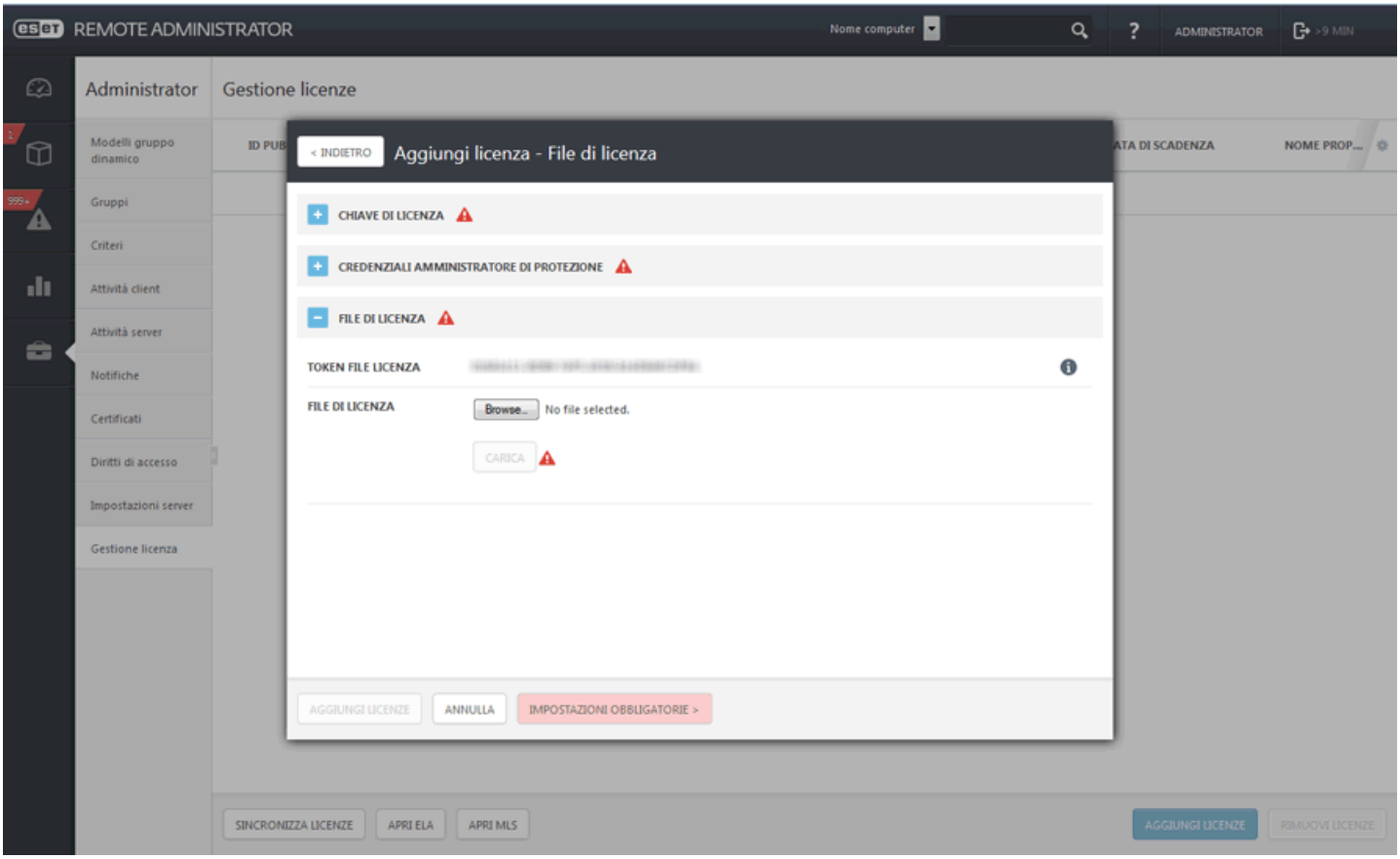
- Digitare o copiare e incollare la **Chiave di licenza** ricevuta all'acquisto della soluzione di protezione ESET nel campo Chiave di licenza. Se si utilizzano credenziali licenza legacy (un nome utente e una password), convertire le credenziali in una chiave di licenza. Se la licenza non è registrata, verrà avviato il processo di registrazione che sarà eseguito sul portale ELA (ERA fornirà l'URL valido per la registrazione in base all'origine della licenza).



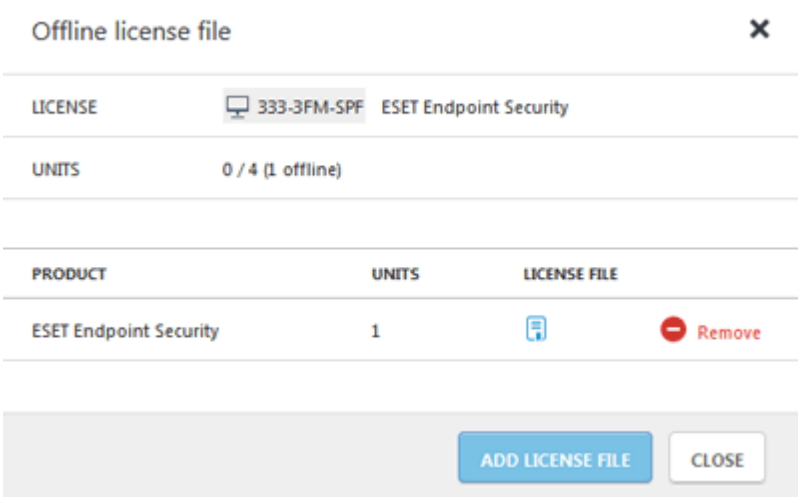
- Immettere le credenziali dell'account **Security Admin** (tutte le licenze delegate saranno successivamente visualizzate in Gestione licenze ERA).



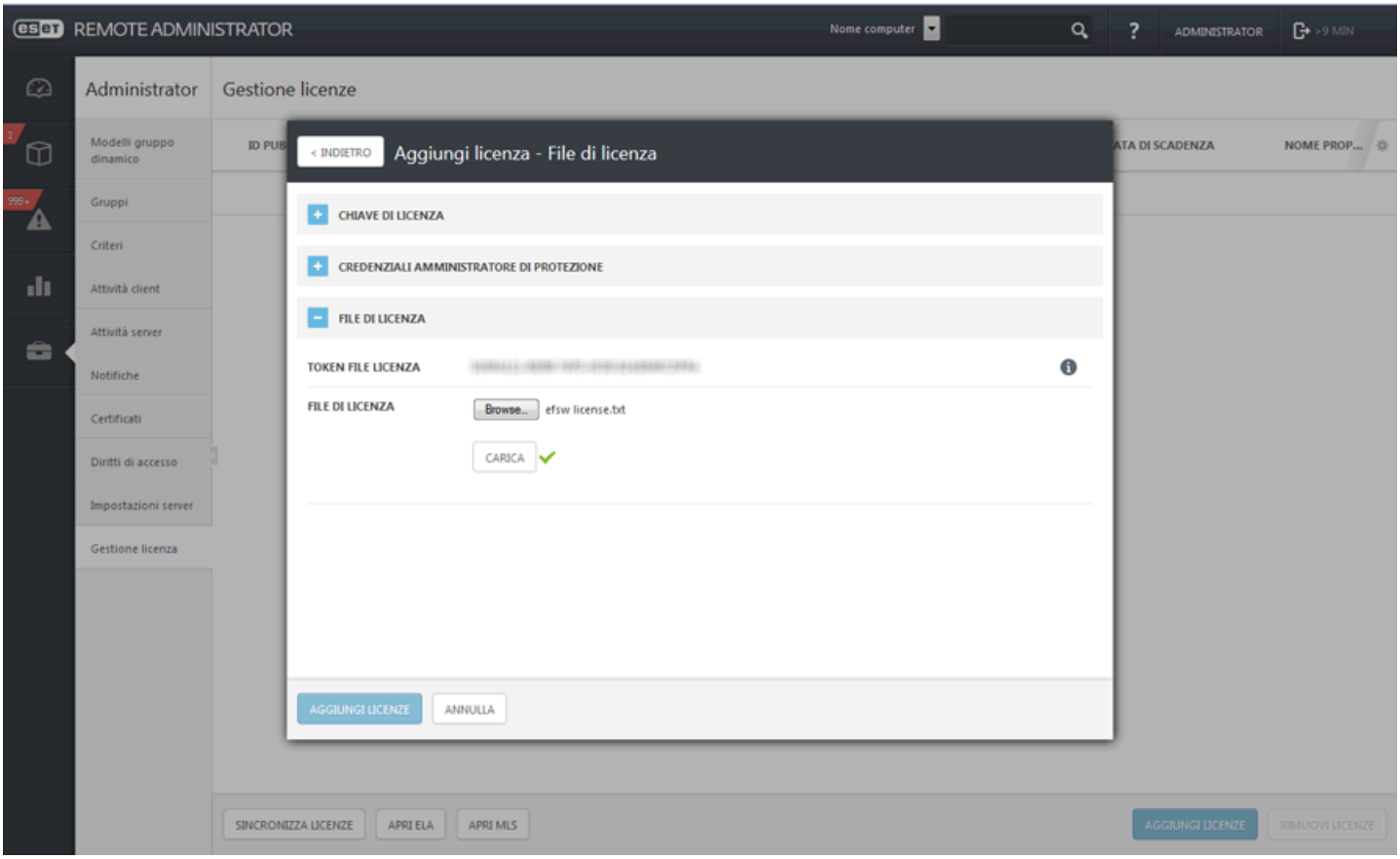
- Immettere il **File di licenza off-line**: sarà necessario eseguire l'esportazione tramite il portale ELA ed includere le informazioni sui prodotti che possono essere gestiti da ERA. Quando si genera un file di licenza off-line sarà necessario immettere un **Token file di licenza** specifico nel portale ESET License Administrator. In caso contrario, il file di licenza non sarà accettato da ESET Remote Administrator.



Fare clic sul simbolo a forma di documento per salvare il file di licenza off-line.



Tornare alla Gestione licenze ERA, fare clic su Aggiungi licenze, quindi su Sfoglia per ricercare il file di licenza off-line esportato in ELA, poi su **Carica**.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Administrator
Gestione licenze
Modelli gruppo dinamico
Gruppi
Criteri
Attività client
Attività server
Notifiche
Certificati
Diritti di accesso
Impostazioni server
Gestione licenza
< INDIETRO
Aggiungi licenza - File di licenza
CHIAVE DI LICENZA
CREDENZIALI AMMINISTRATORE DI PROTEZIONE
FILE DI LICENZA
TOKEN FILE LICENZA
FILE DI LICENZA
Browse...
efsw license.txt
CARICA
AGGIUNGI LICENZE
ANNULLA
SINCRONIZZA LICENZE
APRI ELA
APRI MLS
AGGIUNGI LICENZE
RIMUOVI LICENZE

7. Strumento di diagnostica

Lo strumento di diagnostica è un componente di ERA. utilizzato dagli sviluppatori per la raccolta e la compressione dei rapporti ai fini della risoluzione di problemi relativi ai componenti del prodotto. Eseguire lo Strumento di diagnostica, selezionare una cartella radice in cui verranno salvati i rapporti e le azioni da intraprendere (vedere la sezione **Azioni** sottostante).

Posizione dello **Strumento di diagnostica**:

Windows

Cartella *C:\Program Files\ESET\RemoteAdministrator\<product>*, un file chiamato **Diagnostic.exe**.

Linux

Percorso sul server: */opt/eset/RemoteAdministrator/<product>/*, è presente un eseguibile del **<prodotto> Diagnostic** (una parola, ad esempio **DiagnosticServer**, **DiagnosticAgent**...)

Azioni

- **Rapporti dump**: viene creata una cartella in cui verranno salvati tutti i rapporti.
- **Processo dump**: viene creata una nuova cartella. In caso di rilevamento di un problema, viene creato generalmente un file dump di processo. Se il problema è serio, il sistema creerà un file dump. Per controllarlo manualmente, accedere alla cartella %temp% (su Windows) oppure alla cartella /tmp/ (su Linux) e inserire un file dmp.
  NOTA: il servizio (Agent, Proxy, Server, RD Sensor, FileServer) deve essere in esecuzione.
- **Informazioni generali sull'applicazione**: viene creata la cartella GeneralApplicationInformation e al suo interno il file GeneralApplicationInformation.txt. Il file contiene informazioni testuali tra cui il nome e la versione del prodotto correntemente installato.
- **Configurazione azione**: viene creata una cartella di configurazione in cui verrà salvato il file storage.lua.

8. Glossario

8.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

8.1.1 Virus

Un virus è un'infiltrazione che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili e i documenti. Per replicarsi, un virus allega se stesso all'interno di un file di destinazione. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante tenere presente che i virus (se paragonati a trojan o spyware) sono sempre più rari, poiché non sono commercialmente allettanti per gli autori di software dannosi. Inoltre, il termine "virus" è spesso utilizzato in modo errato per indicare tutti i tipi di infiltrazioni. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare lo stato originale dei file infetti, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: OneHalf, Tenga e Yankee Doodle.

8.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

Tra i worm più noti si segnalano: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

8.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Tuttavia, è importante notare che ciò era vero in passato ma oggi tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "Trojan horse" ("cavallo di Troia") ha assunto un'accezione molto generale che indica un'infiltrazione che non rientra in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader** - Programma dannoso in grado di scaricare altre infiltrazioni da Internet.
- **Dropper** - Tipo di trojan horse concepito per installare sui computer compromessi altri tipi di malware.
- **Backdoor** - Applicazione che comunica con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso a un sistema e assumerne il controllo.
- **Keylogger** - (registratore delle battute dei tasti) - Programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti.
- **Dialer** - Programma progettato per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti la creazione di una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Solitamente, i trojan horse assumono la forma di file eseguibili con estensione .exe. Se sul computer in uso viene rilevato un file classificato come trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

Tra i trojan più noti si segnalano: NetBus, Trojandownloader. Small.ZL, Slapper

8.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file, i dati del registro di Windows, ecc. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1) Quando tentano di accedere a un sistema. Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2) Quando sono nascosti dal normale testing. Gli utenti di ESET Remote Administrator hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

8.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità ("advertising-supported software"). Rientrano in questa categoria i programmi che consentono di visualizzare materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, si rivelano molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non verranno installati senza l'installazione dell'adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, si consiglia di eliminarlo, in quanto esistono elevate probabilità che contenga codice dannoso.

8.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso o la consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

8.1.7 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET Remote Administrator offre la possibilità di rilevare tali minacce.

"Applicazioni potenzialmente pericolose" è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

8.1.8 Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

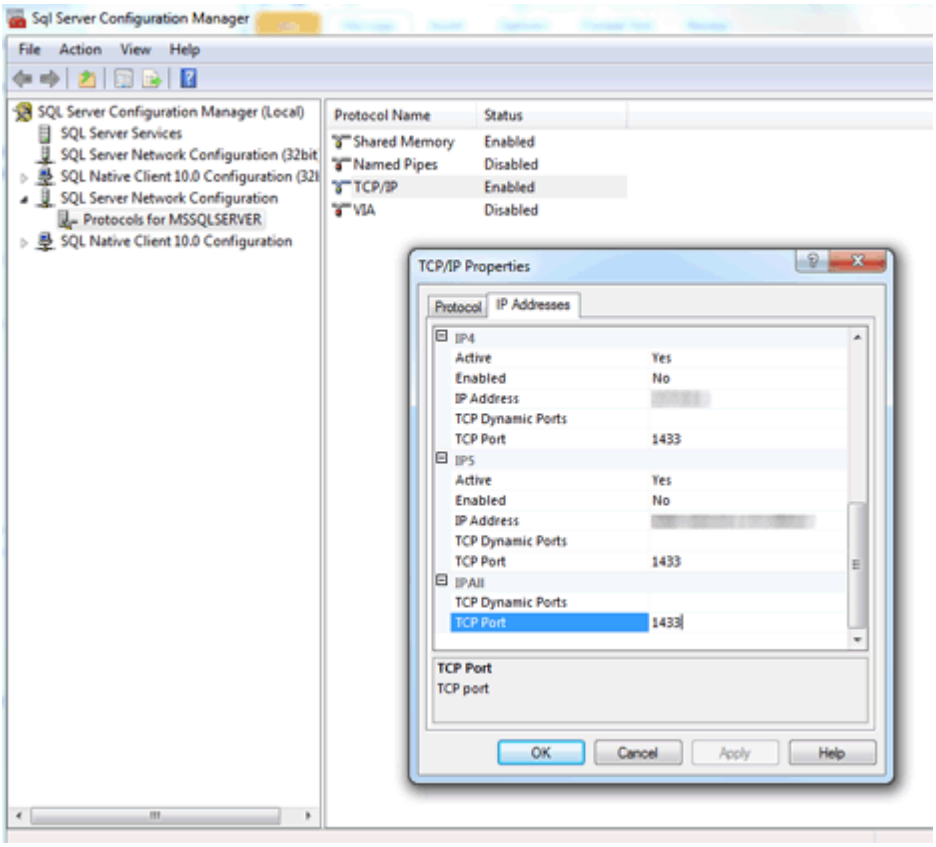
- Nuove finestre aperte mai visualizzate in precedenza
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazioni che comunicano con server remoti

9. Domande frequenti

D: Perché su un server è necessario installare Java? Questa operazione non crea un rischio per la protezione?
R: Per far funzionare correttamente ERA Web Console, è necessario installare Java. Java è uno standard industriale per le console basate sul Web. Sebbene ERA Web Console richieda come requisito minimo Java versione 7, si raccomanda vivamente di utilizzare l'ultima versione di Java rilasciata ufficialmente.

D: Il seguente messaggio di errore viene registrato continuamente nel file trace.log di ESET Rogue Detector:
Informazioni 2015-02-25 18:55:04: CPCAPDeviceSniffer [Thread 764]: CPCAPDeviceSniffer on rpcap://\Device \NPF_{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} errore generato: Si è verificato un errore durante l'apertura del dispositivo:errore durante l'apertura dell'adattatore: Il sistema non ha trovato il dispositivo specificato. (20)
R: Questo è un problema che si verifica con WinPcap: interrompere il servizio ESET Rogue Detector Sensor, reinstallare l'ultima versione di WinPcap (versione minima: 4.1.0) e riavviare il servizio ESET Rogue Detector Sensor.

D: Dove è possibile recuperare agevolmente il numero di porta di SQL Server?
R: Esistono vari modi per determinare il numero della porta SQL. Per ottenere risultati più accurati, è possibile utilizzare SQL Server Configuration Manager. Consultare l'immagine sottostante per visualizzare un esempio che illustra il punto in cui queste informazioni sono disponibili in SQL Server Configuration Manager:



D: Dopo aver installato SQL Express 2008 (incluso nel pacchetto ERA) su Windows Server 2012, sembra che l'applicazione non sia in ascolto su una porta SQL standard.
R: È molto probabile che sia in ascolto su una porta diversa da quella predefinita, ovvero la 1433.

D: In che modo è possibile configurare MySQL per poter accettare pacchetti di grandi dimensioni?
R: Individuare il file di configurazione MySQL (**my.ini** per Windows e **my.cnf** per Linux, la posizione esatta del file .ini potrebbe differire da un sistema operativo a un altro), aprirlo e ricercare la sezione `[mysqld]`. Aggiungere una nuova riga `max_allowed_packet=33M` (il valore deve avere una dimensione minima di 33 M).

D: In caso di installazione SQL da parte dell'utente, in che modo è possibile creare un database per ERA?
R: Non è necessario farlo. Il database viene creato **dal** programma di installazione Server.msi, non dal programma di installazione ERA. Il programma di installazione ERA consente di semplificare la procedura per l'utente: questo elemento, infatti, installa il SQL Server, mentre il database viene creato dal programma di installazione server.msi.

D: Il programma di installazione ERA è in grado di creare un nuovo database al posto dell'utente in un'installazione SQL Server esistente, se vengono forniti i dettagli e le credenziali corretti relativi alla connessione? Sarebbe preferibile che il programma di installazione supportasse varie versioni di SQL Server (2008, 2014, ecc.)
R: Il database viene creato da **Server.msi**. Di conseguenza, il programma di installazione è in grado di creare un database ERA al posto dell'utente su istanze di SQL Server installate in modo autonomo. Esatto, le versioni supportate di SQL Server sono 2008, 2012 e 2014.

D: Perché la versione SQL 2008 R2 viene utilizzata nel programma di installazione ERA?
R: Viene utilizzata la versione SQL 2008 R2 in quanto Microsoft dichiara la compatibilità per questo tipo di database su Windows XP e sui sistemi operativi successivi.

D: Cosa fare se si riceve un **codice di errore: -2068052081** durante l'installazione di MSSQL?
R: Riavviare il computer ed eseguire nuovamente la configurazione. Se il problema persiste, disinstallare il client nativo di SQL Server ed eseguire nuovamente l'installazione. Se il problema persiste, disinstallare tutti i prodotti di Microsoft SQL Server, riavviare il computer ed eseguire nuovamente l'installazione.

D: Cosa fare se si riceve un **codice di errore: -2067922943** durante l'installazione di MSSQL?
R: Assicurarsi che il sistema soddisfi i requisiti del database per ERA.

D: In caso di installazione su un SQL Server esistente, per impostazione predefinita verrà utilizzata la modalità di autenticazione di Windows integrata?
R: No, perché la modalità di autenticazione di Windows può essere disattivata su SQL Server e l'unico modo per accedere consiste nell'utilizzare l'autenticazione di SQL Server (inserendo un nome utente e una password). È necessario utilizzare l'autenticazione di SQL Server o la modalità mista. In caso di installazione manuale di SQL Server, si consiglia di creare una password radice per SQL Server (l'utente radice è chiamato "sa", che sta per "security admin") e di conservarla in un luogo sicuro per consultazioni successive. Durante l'aggiornamento del server ERA, potrebbe essere necessario inserire la password radice.

D: È stato necessario installare **Microsoft .NET Framework 3.5** perché il programma di installazione ERA ha puntato l'utente (http://www.microsoft.com/en-us/download/details.aspx?id=21), ma non ha funzionato su una nuova installazione di Windows Server 2012 R2 con SP1.
R: Non è possibile utilizzare questo programma di installazione su Windows Server 2012, a causa del criterio di protezione su Windows Server 2012. Microsoft .NET Framework deve essere installato mediante **la Procedura guidata regole e funzioni.**.

D: Microsoft .NET 4.5 framework era già installato sul sistema in uso. Per aggiungere .NET 3.5., è stato necessario installare la Procedura guidata regole e funzioni. Perché non funziona sulla versione 4.5?
R: Perché .NET 4.5 non possiede una compatibilità retroattiva con .NET 3.5., che è un prerequisito del programma di installazione di SQL Server.

D: È estremamente complesso capire se l'installazione di SQL Server è in esecuzione. Come è possibile capire cosa succede se l'installazione dura più di 10 minuti?
R: Raramente, l'installazione di SQL Server può richiedere fino a 1 ora. I tempi di installazione dipendono dalle prestazioni del sistema.

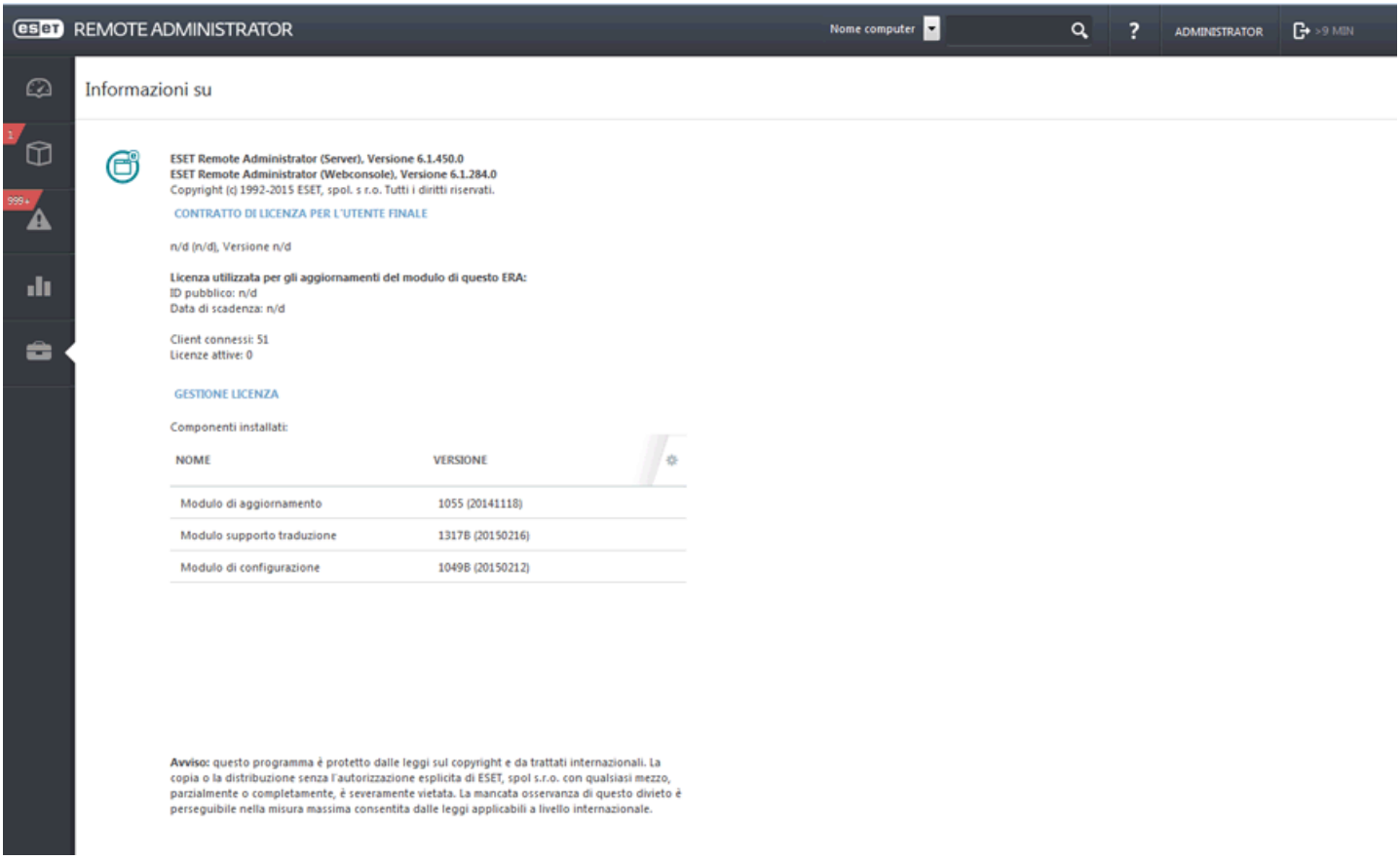
D: In che modo è possibile **ripristinare la password dell'amministratore** per la console Web (inserita durante la configurazione)?
R: È possibile reimpostare la password scegliendo **Ripara** durante l'esecuzione del programma di installazione del server. Tuttavia, potrebbe essere necessario inserire la password del database ERA in caso di mancato utilizzo dell'autenticazione di Windows durante la creazione del database.

NOTA: Prestare attenzione al fatto che alcune opzioni di riparazione potrebbero determinare la rimozione dei dati archiviati.

D: Qual è il formato da utilizzare per l'importazione di un file contenente un elenco di computer da aggiungere a ERA?
R: File contenente le seguenti righe:
All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX
Tutti è il nome richiesto del gruppo radice.

10. Informazioni su ESET Remote Administrator

In questa finestra vengono fornite informazioni dettagliate sulla versione installata di ESET Remote Administrator e un elenco dei moduli del programma installati. Nella parte superiore, sono visualizzate le informazioni sul sistema operativo e sulle risorse di sistema.


REMOTE ADMINISTRATOR
Nome computer
ADMINISTRATOR
Informazioni su
ESET Remote Administrator (Server), Versione 6.1.450.0
ESET Remote Administrator (Webconsole), Versione 6.1.284.0
Copyright (c) 1992-2015 ESET, spol. s r.o. Tutti i diritti riservati.
CONTRATTO DI LICENZA PER L'UTENTE FINALE
n/d (n/d), Versione n/d
Licenza utilizzata per gli aggiornamenti del modulo di questo ERA:
ID pubblico: n/d
Data di scadenza: n/d
Client connessi: 51
Licenze attive: 0
GESTIONE LICENZA
Componenti installati:
NOME
VERSIONE
Modulo di aggiornamento
1055 (20141118)
Modulo supporto traduzione
1317B (20150216)
Modulo di configurazione
1049B (20150212)
Avviso: questo programma è protetto dalle leggi sul copyright e da trattati internazionali. La copia o la distribuzione senza l'autorizzazione esplicita di ESET, spol s.r.o. con qualsiasi mezzo, parzialmente o completamente, è severamente vietata. La mancata osservanza di questo divieto è perseguibile nella misura massima consentita dalle leggi applicabili a livello internazionale.

11. Accordo di licenza per l'utente finale (ALUF)

IMPORTANTE: leggere attentamente i termini e le condizioni delineati di seguito prima di scaricare, installare, copiare o utilizzare il prodotto. **SCARICANDO, INSTALLANDO, COPIANDO O UTILIZZANDO IL SOFTWARE, L'UTENTE SI IMPEGNA AD ACCETTARE I TERMINI E LE CONDIZIONI DEL PRESENTE ACCORDO**.

Accordo di licenza per l'utente finale del software.

Ai sensi del presente Accordo di licenza per l'utente finale (qui di seguito denominato "Accordo"), stipulato da e tra ESET, spol. s r. o., con sede legale presso Einsteinova 24, 851 01 Bratislava, Repubblica Slovacca, iscritta nel registro delle imprese di competenza del tribunale circoscrizionale Bratislava I, Sezione Sro, numero di registro 3586/B, numero di identificazione commerciale: 31 333 535 o un'altra società del gruppo ESET (qui di seguito denominata "ESET" o "Fornitore") e l'utente, ovvero una persona fisica o giuridica (qui di seguito denominato "Utente" o "Utente finale"), l'Utente ha facoltà di utilizzare il Software specificato all'Articolo 1 del presente Accordo. Il Software specificato all'Articolo 1 del presente Accordo può essere memorizzato su un supporto informatico, inviato tramite posta elettronica, scaricato da Internet, scaricato dai server del Fornitore o ottenuto da altre fonti secondo i termini e le condizioni specificati di seguito.

IL PRESENTE ACCORDO HA PER OGGETTO I DIRITTI DELL'UTENTE FINALE E NON COSTITUISCE UN CONTRATTO DI VENDITA. Il Fornitore conserva la proprietà della copia del Software e dei supporti fisici contenuti nella confezione di vendita, nonché di ogni altra copia che l'Utente finale è autorizzato a effettuare in conformità al presente Accordo.

Facendo clic sul pulsante "Accetto" durante l'installazione, il download, la copia o l'utilizzo del Software, l'Utente accetta i termini e le condizioni del presente Accordo. Se l'Utente non intende accettare integralmente i termini e le condizioni del presente Accordo, deve prontamente fare clic sull'opzione "Non accetto", interrompere l'installazione o il download oppure eliminare o restituire il Software, i supporti di installazione, la documentazione di accompagnamento e la ricevuta dell'acquisto a ESET o presso il punto vendita in cui l'Utente ha acquistato il Software.

L'UTENTE CONVIENE CHE IL SUO UTILIZZO DEL SOFTWARE COSTITUISCE CONFERMA DELL'AVVENUTA LETTURA, COMPRENSIONE E ACCETTAZIONE DEL PRESENTE ACCORDO E ACCETTA DI RISPETTARE I TERMINI E LE CONDIZIONI INDICATI.

1. **Software**. Ai sensi del presente Accordo, il termine "Software" indica: (i) il programma ESET Remote Administrator e tutti i suoi componenti; (ii) tutti i contenuti presenti su dischi, CD-ROM, DVD, posta elettronica ed eventuali allegati, nonché altri supporti multimediali tramite i quali viene fornito il presente Accordo, inclusa la versione del Software in codice oggetto fornita su un supporto informatico, tramite posta elettronica o scaricata da Internet; (iii) istruzioni scritte ed eventuale documentazione correlata al Software, in particolare qualsiasi descrizione del Software, delle relative specifiche, qualsiasi descrizione delle proprietà o del funzionamento del Software, qualsiasi descrizione dell'ambiente operativo di utilizzo del Software, istruzioni per l'uso o l'installazione del Software o qualsiasi descrizione della modalità di utilizzo del Software (qui di seguito denominata "Documentazione"); (iv) copie del Software, patch per eventuali errori del Software, aggiunte o estensioni, versioni modificate del Software, nonché gli aggiornamenti dei componenti del Software, se forniti, concessi in licenza all'Utente finale dal Fornitore ai sensi dell'Articolo 3 del presente Accordo. Il Software deve essere fornito esclusivamente sotto forma di codice oggetto eseguibile.

2. **Installazione**. Il Software fornito su un supporto informatico, inviato tramite posta elettronica, scaricato da Internet o dai server del Fornitore o ottenuto da altre fonti richiede una procedura di installazione. L'Utente deve installare il Software su un computer correttamente configurato, conformemente ai requisiti specificati nella Documentazione fornita. Il metodo di installazione è illustrato nella Documentazione. È vietato installare programmi per computer o componenti hardware che possono influire negativamente sul Software sullo stesso computer su cui si installa il Software medesimo.

3. **Licenza**. Posto che l'Utente abbia accettato i termini del presente Accordo, versato il corrispettivo relativo alla Tariffa di licenza entro il periodo di scadenza e rispettato tutti i termini e le condizioni ivi indicati, il Fornitore deve garantire all'Utente i seguenti diritti ("Licenza"):

a) **Installazione e utilizzo**. L'Utente avrà un diritto non esclusivo e non trasferibile per l'installazione del Software sul disco rigido di un computer o su altri supporti permanenti per la memorizzazione dei dati, l'installazione e la memorizzazione del Software sulla memoria di un computer e per l'implementazione, la memorizzazione e la visualizzazione del Software.

b) **Indicazione del numero di licenze**. Il diritto di utilizzare il Software è vincolato al numero di Utenti finali. Quanto segue fa riferimento a un Utente finale: (i) installazione del Software su un computer, o (ii) se una licenza è legata al numero di caselle di posta, un Utente finale corrisponderà a un utente che accetta la posta elettronica tramite un Mail User Agent (qui di seguito denominato "MUA"). Se un MUA accetta la posta elettronica e successivamente la distribuisce automaticamente a diversi utenti, il numero di Utenti finali sarà determinato in base al numero effettivo di utenti a cui viene distribuita la posta elettronica. Se un server di posta svolge la funzione di Mailgate, il numero di Utenti finali dovrà essere pari al numero di utenti del server di posta per cui tale gate fornisce i servizi. Se un numero non specificato di indirizzi di posta elettronica è diretto a e accettato da un utente (ad esempio attraverso alias) e i messaggi non sono automaticamente distribuiti dal client a un numero maggiore di utenti, è richiesta una Licenza per un computer soltanto. L'Utente non deve utilizzare la stessa Licenza contemporaneamente su più di un computer.

c) **Business Edition**. Occorre ricevere una versione Business Edition del Software per utilizzare il Software su server di posta, mail relay, gateway di posta o gateway Internet.

d) **Termine della Licenza**. Il diritto di utilizzo del Software deve essere limitato nel tempo.

e) **Software OEM**. Il software OEM deve essere limitato al computer con il quale è stato ricevuto. Non è possibile trasferirlo su un computer diverso

f) **Versione di valutazione ("NFR") e versione di prova**. Il software classificato come "Not-for-resale" ("NFR", versione di valutazione) o di prova ("TRIAL") è gratuito e deve essere utilizzato esclusivamente ai fini della verifica e della valutazione delle funzioni del Software.

g) **Risoluzione della Licenza**. La Licenza scadrà automaticamente al termine del periodo stabilito. In caso di mancato rispetto di qualsiasi clausola del presente Accordo, il Fornitore è autorizzato a recedere dall'Accordo, senza pregiudizio per i diritti o i rimedi giuridici in capo al Fornitore in tali eventualità. In caso di annullamento della Licenza, l'Utente è tenuto a eliminare, distruggere o restituire immediatamente e a proprie spese il Software e tutte le copie di backup a ESET o presso il punto vendita in cui ha ottenuto il Software.

4. **Connessione a Internet**. Per il corretto funzionamento, il Software richiede una connessione a Internet e deve essere collegato a intervalli regolari ai server del Fornitore o di terzi. La connessione a Internet è necessaria per le seguenti funzioni del Software:

a) **Aggiornamenti del Software**. Il Fornitore è autorizzato, ma non obbligato, a rilasciare di tanto in tanto aggiornamenti del Software ("Aggiornamenti"). Questa funzione è abilitata nelle impostazioni standard del Software e gli Aggiornamenti vengono pertanto installati automaticamente, eccetto nel caso in cui l'Utente finale abbia disattivato l'installazione automatica degli Aggiornamenti.

b) **Inoltro di infiltrazioni e di informazioni al Fornitore**. Il Software prevede una funzione in grado di raccogliere campioni di nuovi virus, di altri programmi dannosi simili e di file sospetti o problematici (qui di seguito denominati "Infiltrazioni") e di inviarli al Fornitore, insieme alle informazioni relative al computer e/o alla piattaforma su cui è installato il Software (qui di seguito denominate "Informazioni"). Le Informazioni possono contenere dati (compresi dati personali) sull'Utente finale e/o su altri utenti del computer su cui è installato il Software, informazioni sul computer, sul sistema operativo e sui programmi installati, sui file del computer su cui è installato il Software e sui file contenenti un'Infiltrazione. Il Fornitore dovrà utilizzare esclusivamente le Informazioni e le Infiltrazioni ricevute per la ricerca di Infiltrazioni e dovrà adottare misure appropriate per garantire la riservatezza delle Informazioni ricevute. Accettando il presente Accordo e attivando la funzione del software descritta in precedenza, l'Utente accetta che le Infiltrazioni e le Informazioni vengano inviate al Fornitore e garantisce altresì al Fornitore l'approvazione necessaria, ai sensi delle normative vigenti, per l'elaborazione delle Informazioni ottenute.

5. **Esercizio dei diritti dell'Utente finale**. L'Utente deve esercitare i diritti dell'Utente finale di persona o attraverso i propri dipendenti. L'Utente è autorizzato a utilizzare il Software al solo scopo di salvaguardare le proprie operazioni e proteggere i computer per cui è stata ottenuta la Licenza.

6. **Limitazioni dei diritti**. Sono vietate la copia, la distribuzione, la separazione dei componenti e la creazione di prodotti derivati del Software. Durante l'utilizzo del Software, l'Utente è tenuto ad attenersi alle seguenti limitazioni:

(a) È autorizzata una copia del Software su supporti di archiviazione permanente come copia di backup, a condizione che quest'ultima non venga installata o utilizzata su altri computer. Ogni altra copia del Software effettuata dall'Utente rappresenta una violazione del presente Accordo.

(b) L'Utente non può utilizzare, modificare, tradurre o riprodurre il Software, né trasferire i diritti all'utilizzo del Software, né copiare il Software, eccetto laddove espressamente indicato nel presente Accordo.

(c) La rivendita, la sublicenza, il noleggio, il prestito o l'utilizzo del Software per la fornitura di servizi commerciali non sono consentiti.

(d) Sono vietate la decodificazione, la decomposizione o il disassemblaggio del Software o qualsivoglia tentativo di determinazione del codice sorgente del software, fatto salvo laddove tale divieto è espressamente proibito per legge.

(e) L'Utente accetta di utilizzare il Software esclusivamente secondo modalità conformi a tutte le leggi applicabili nella giurisdizione in cui avviene l'utilizzo dello stesso, incluse, a titolo esemplificativo ma non esaustivo, le limitazioni relative al copyright e ad altri diritti sulla proprietà intellettuale.

7. **Copyright**. Il Software e tutti i relativi diritti, inclusi, a titolo esemplificativo ma non esaustivo, i diritti di esclusiva e i diritti di proprietà intellettuale associati, appartengono a ESET e/o ai suoi licenziatari. e sono protetti dalle disposizioni dei trattati internazionali, nonché da ogni altra legge nazionale applicabile nel paese di utilizzo del Software. La struttura, l'organizzazione e il codice del Software costituiscono preziosi segreti commerciali e dati sensibili di proprietà di ESET e/o dei suoi licenziatari. È vietata la copia del Software, fatta eccezione per i casi previsti all'Articolo 6(a). Ogni copia autorizzata ai sensi del presente Accordo deve contenere gli stessi avvisi sul copyright e sulla proprietà riportati sul Software. Se l'Utente effettua la decodificazione, la decompilazione, il disassemblaggio o qualsivoglia tentativo di determinazione del codice sorgente in violazione delle disposizioni del presente Accordo, qualsiasi informazione in tal modo ottenuta sarà irrevocabilmente e automaticamente ritenuta trasferita al Fornitore e di completa proprietà del Fornitore dal momento della sua origine, fermi restando i diritti del Fornitore relativi alla violazione del presente Accordo.

8. **Riserva di diritti**. Il Fornitore si riserva tutti i diritti relativi al Software, fatta eccezione per quelli espressamente concessi all'Utente finale nel presente Accordo.

9. **Versioni in più lingue, software su due supporti, duplicati**. Se il Software supporta più piattaforme o lingue o se l'Utente ha ricevuto più copie del Software, questi è autorizzato a utilizzare il Software unicamente per il numero di computer e per le versioni per i quali ha ottenuto una Licenza. La vendita, il noleggio, l'affitto, la sublicenza, il prestito o il trasferimento di versioni o copie del Software non utilizzate dall'Utente non sono consentiti.

10. **Entrata in vigore e risoluzione dell'Accordo**. Il presente Accordo entra in vigore alla data dell'accettazione dei termini dell'Accordo medesimo da parte dell'Utente. Quest'ultimo potrà recedere dall'Accordo in qualsiasi momento disinstallando, distruggendo e restituendo, in modo permanente e a sue spese, il Software, tutte le copie di backup e tutto il materiale correlato ricevuto dal Fornitore o dai suoi partner commerciali. Indipendentemente dalla modalità di risoluzione del presente Accordo, le disposizioni previste agli Articoli 7, 8, 11, 13, 20 e 22 resteranno valide senza limiti di tempo.

11. **DICHIARAZIONI DELL'UTENTE FINALE**. L'UTENTE FINALE RICONOSCE CHE IL SOFTWARE VIENE FORNITO "COSÌ COM'È", SENZA GARANZIE DI ALCUN TIPO, NÉ ESPLICITE NÉ IMPLICITE, E CHE, SALVO QUANTO INDEROGABILMENTE PREVISTO DALLA LEGGE, IL FORNITORE, I SUOI LICENZIATARI O AFFILIATI COME ANCHE I TITOLARI DEL COPYRIGHT, NON RILASCIANO ALCUNA DICHIARAZIONE O GARANZIA ESPLICITA O IMPLICITA, COMPRESE, A TITOLO ESEMPLIFICATIVO MA NON ESAUSTIVO, GARANZIE DI COMMERCIABILITÀ O IDONEITÀ PER UN FINE PARTICOLARE O LA GARANZIA CHE IL SOFTWARE NON VIOLI BREVETTI, COPYRIGHT, MARCHI O ALTRI DIRITTI DI TERZE PARTI. IL FORNITORE O ALTRE PARTI NON GARANTISCONO CHE LE FUNZIONI CONTENUTE NEL SOFTWARE SODDISFERANNO I REQUISITI DELL'UTENTE, NÉ CHE L'USO DEL SOFTWARE NON SUBIRÀ INTERRUZIONI O CHE LO STESSO SIA ESENTE DA ERRORI. L'UTENTE SI ASSUME TUTTE LE RESPONSABILITÀ E I RISCHI PER LA SCELTA DEL SOFTWARE AL FINE DI OTTENERE I RISULTATI DESIDERATI, NONCHÉ PER L'INSTALLAZIONE, L'UTILIZZO E I RISULTATI OTTENUTI DALL'UTILIZZO DEL SOFTWARE.

12. **Assenza di altri obblighi**. Il presente Accordo non pone in essere altri obblighi a carico del Fornitore e dei suoi licenziatari oltre a quanto ivi specificatamente stabilito.

13. **LIMITAZIONE DI RESPONSABILITÀ**. NELLA MISURA MASSIMA CONSENTITA AI SENSI DI LEGGE, IN NESSUNA CIRCOSTANZA IL FORNITORE, I SUOI DIPENDENTI O LICENZIATARI POTRANNO ESSERE RITENUTI RESPONSABILI PER LUCRO CESSANTE, PERDITA DI RICAVI, VENDITE, DATI O PER COSTI DERIVANTI DALLA SOSTITUZIONE DI BENI O SERVIZI, DANNI ALLA PROPRIETÀ, LESIONI PERSONALI, INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, SMARRIMENTO DI INFORMAZIONI COMMERCIALI, O PER QUALSIASI DANNO SPECIALE, DIRETTO, INDIRETTO, ACCIDENTALE, ECONOMICO, ESEMPLARE, PUNITIVO O CONSEQUENZIALE, INDIPENDENTEMENTE DALLA CAUSA E DAL FATTO CHE TALE EVENTO DERIVI DA CONTRATTO, FATTO ILLECITO, NEGLIGENZA O ALTRA INTERPRETAZIONE DI RESPONSABILITÀ DERIVANTE DALL'UTILIZZO OPPURE DALL'IMPOSSIBILITÀ DI UTILIZZARE IL SOFTWARE, ANCHE QUALORA IL FORNITORE O I SUOI LICENZIATARI O AFFILIATI SIANO STATI AVVISATI DELLA POSSIBILITÀ DI TALI DANNI. POICHÉ ALCUNI PAESI E GIURISDIZIONI NON AMMETTONO L'ESCLUSIONE DI RESPONSABILITÀ, MA POTREBBERO CONSENTIRNE UNA LIMITAZIONE, IN QUESTI CASI LA RESPONSABILITÀ DEL FORNITORE, DEI SUOI DIPENDENTI O LICENZIATARI O AFFILIATI SARÀ LIMITATA AL PREZZO CORRISPOSTO PER L'ACQUISTO DELLA LICENZA.

14. Nessuna disposizione contenuta nel presente Accordo costituirà pregiudizio per i diritti legali di qualsiasi parte in veste di consumatore in caso di funzionamento contrario a quanto esposto.

15. **Supporto tecnico**. ESET o terze parti commissionate da ESET forniranno supporto tecnico a propria discrezione, senza garanzie né dichiarazioni. Verrà richiesto all'Utente finale di salvare tutti i dati, i software e i programmi prima della fornitura del supporto tecnico. ESET e/o terze parti commissionate da ESET non possono accettare la responsabilità per danni o perdite di dati, proprietà, software o hardware o perdita di profitti legati alla fornitura del supporto tecnico. ESET e/o terze parti commissionate da ESET si riservano il diritto di decidere che la risoluzione del problema vada al di là dell'ambito di competenza del supporto tecnico. ESET si riserva il diritto di rifiutare, interrompere o concludere la fornitura del supporto tecnico a sua discrezione.

16. **Trasferimento della Licenza**. È possibile trasferire il Software da un computer a un altro, eccetto se in contrasto con i termini dell'Accordo. Se non in contrasto con i termini dell'Accordo, l'Utente finale sarà autorizzato a trasferire permanentemente la Licenza e tutti i diritti derivanti dal presente Accordo a un altro Utente finale con il consenso del Fornitore, secondo la condizione che (i) l'Utente finale originale non conservi copie del Software; (ii) il trasferimento dei diritti sia diretto, ossia dall'Utente finale originale al nuovo Utente finale; (iii) il nuovo Utente finale si assuma tutti i diritti e gli obblighi incombenti sull'Utente finale originale secondo i termini del presente Accordo; (iv) l'Utente finale originale fornisca al nuovo Utente finale la documentazione che consente la verifica dell'autenticità del Software, come specificato all'Articolo 17.

17. **Verifica dell'autenticità del Software**. L'Utente finale può dimostrare il diritto a utilizzare il Software in uno dei modi seguenti: (i) tramite un certificato di licenza emesso dal Fornitore o da terzi designati dal Fornitore; (ii) tramite un contratto di licenza scritto, se tale contratto è stato stipulato; (iii) tramite l'invio di un'e-mail da parte del Fornitore contenente i dettagli della licenza (nome utente e password) per l'attivazione degli Aggiornamenti.

18. **Dati sull'Utente finale e protezione dei diritti**. L'Utente finale autorizza il Fornitore a trasferire, elaborare e salvare i dati di identificazione dell'Utente medesimo. L'Utente accetta che il Fornitore verifichi con i propri mezzi la conformità dell'utilizzo del Software alle disposizioni previste dal presente Accordo. L'utente accetta il trasferimento di dati, attraverso la comunicazione del Software con i sistemi informatici del Fornitore o dei relativi partner commerciali, ai fini della garanzia della funzionalità e dell'autorizzazione all'utilizzo del Software, nonché della protezione dei diritti del Fornitore. Alla risoluzione del presente Accordo, il Fornitore o qualsiasi suo partner commerciale deve essere autorizzato al trasferimento, all'elaborazione e alla memorizzazione dei dati fondamentali che identificano l'Utente, a scopo di fatturazione e ai fini dell'esecuzione del presente Accordo. Ulteriori informazioni sulla tutela della privacy e dei dati personali sono disponibili all'indirizzo http://www.eset.it/supporto/informativa-privacy.

19. **Licenze per enti pubblici e governo degli Stati Uniti**. Il Software sarà fornito agli enti pubblici, incluso il governo degli Stati Uniti, con i diritti e le limitazioni della licenza descritti nel presente Accordo.

20. **Controllo delle esportazioni e delle riesportazioni**. Il Software, la Documentazione o parti di essa, incluse le informazioni sul Software e i rispettivi componenti, sono soggetti a controlli sulle importazioni e sulle esportazioni previsti dalle normative emesse dai governi competenti, incluse le normative sull'amministrazione delle esportazioni degli Stati Uniti. e le limitazioni sull'utilizzo finale e la destinazione emesse dal governo degli Stati Uniti e da altri governi. L'Utente accetta di rispettare rigorosamente tutti i regolamenti applicabili sulle importazioni e sulle esportazioni e riconosce la propria responsabilità nell'ottenere licenze di esportazione, riesportazione, trasferimento o importazione del Software.

21. **Avvisi**. Tutti gli avvisi e i resi del Software e della Documentazione devono essere inviati a: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Repubblica Slovacca.

22. **Legge applicabile**. Il presente Accordo è disciplinato e interpretato in base alle leggi in vigore nella Repubblica Slovacca. L'Utente finale e il Fornitore ivi accettano che gli eventuali conflitti di legge e la Convenzione delle Nazioni Unite sui contratti per la compravendita internazionale di merci non sono applicabili. L'Utente accetta espressamente che qualsiasi reclamo o disputa derivante dal presente Accordo con il Fornitore o correlata all'utilizzo del Software sia di competenza del Tribunale di Bratislava I e accetta espressamente l'esercizio della giurisdizione da parte del suddetto tribunale.

23. **Disposizioni generali**. Qualora alcune disposizioni del presente Accordo fossero giudicate non valide o non applicabili, ciò non avrà alcun effetto sulla parte restante dell'Accordo, che resterà valido e applicabile nei termini e nelle condizioni ivi indicati. Il presente Accordo potrà essere modificato solo in forma scritta e con la firma di un rappresentate autorizzato del Fornitore o di una persona espressamente autorizzata a tale scopo nei termini di una procura.

Il presente Accordo rappresenta l'intero patto stipulato tra l'Utente e il Fornitore in relazione al Software e destituisce di fondamento ogni eventuale rappresentazione, discussione, impegno, comunicazione o avviso precedente relativo al Software.